

Japanese Patent Laid-open No. 2000-293936 A

Publication date : Oct. 20, 2000

Applicant : Hitachi Ltd.

Title : DIGITAL SIGNAL RECORDING APPARATUS, REPRODUCING  
5 APPARATUS, AND RECORDING MEDIUM

[0012] Embodiments of the present invention will be explained below with reference to the accompanying drawings.

10 [0013] Fig. 1 is a configuration diagram including a digital broadcast receiver and a digital signal recording and reproducing apparatus. 200 is a digital signal recording and reproducing apparatus, 201 is a digital broadcast receiving apparatus, 202 is an antenna, 207 is a  
15 receiver, 203 is a tuner, 204 is a selection circuit, 205 is a decryption circuit, 206 is an interface circuit, and 208 is a control circuit for controlling operations of the digital broadcast receiver 201. Although the digital broadcast receiver 201 and the digital recording and  
20 reproducing apparatus 200 are shown as being separate, they can be integrated.

[0014] Fig. 2 is a configuration diagram of the digital signal recording and reproducing apparatus 200 in Fig. 1. Although the apparatus in Fig. 2 is used for both recording  
25 and reproducing, it is the same even if the recording and reproducing are configured to be independent. 100 is a rotating head, 101 is a capstan, 102a is a recording signal processing circuit for performing generation or the like of a recording signal at the time of recording, 102b is a  
30 reproduction signal processing circuit for demodulation or the like of the reproduction signal at the time of reproduction, 104 is a control circuit, for example, like a microprocessor, which controls of the recording and

**THIS PAGE BLANK (USPTO)**

reproduction modes or the like, 105 is a timing generation circuit for generating a timing signal that becomes the reference for rotation of the rotating head 100 or the like, 106 is a servo circuit for controlling the rotating head and the feed speed of the tape, 107 is an input and output circuit for inputting the recording signal or outputting the reproduction signal, 109 is a timing control signal for controlling the timing at the time of recording, 110 is an oscillating circuit for generating a reference clock, 111 is a tape, 112 is a recording and reproduction circuit of the analog video signals, 115 is a data encryption circuit at the time of digital signal recording, 116 is a data decryption circuit at the time of digital signal reproduction, 117 is a device key generator for generating a device key that becomes the basis of the data key that is supplied to the data encryption circuit 115 or a data decryption circuit 116 when digital information is encrypted or decrypted, 118 is a block key generator for generating the block key that is another basis of the data key when digital information is encrypted or decrypted, and 119 is an input and output control circuit for performing time stamp processing of packet data at the time of recording and for performing output control of the packet data at the time of reproduction.

[0015] The digital video compressed signal is sent as packet data by time-division multiplexing the signals of multiple channels. In Fig. 1, the digital broadcasting signal received by the antenna 202 is demodulated by the tuner 203, and then the necessary digital compressed image signal is selected by the selection circuit 204. The selected digital compressed image signal is decrypted into a normal video signal by the decryption circuit 205 and inputted into the receiver 207. When processing such as

**THIS PAGE BLANK (USPTO)**

scrambling or the like is performed on the reception signal, decryption processing is performed in the selection circuit 204 after a process such as scrambling or the like is cancelled. When recording of the received digital broadcast signal is performed, the digital compressed video signal to be recorded and information relating thereto are selected in the selection circuit 204, inputted into the digital signal recording and reproducing apparatus 200 by the input and output terminal 108 of the digital signal recording and reproduction apparatus via the interface circuit 206 and recorded. When reproduction of the recorded digital broadcast signal is performed, the digital compressed image signal or the like reproduced by the digital signal recording and reproduction apparatus 200 is outputted to the interface circuit 206 by the input and output terminal 108. Processes similar to those normally performed at the time of reception are performed on the digital compressed video signal or the like inputted into the interface circuit 106 by the selection circuit and the decryption circuit, and the digital compressed video signal is then outputted to the receiver 207.

[0016] In Fig. 2, which depicts the configuration of the digital signal recording and reproducing apparatus 200 in Fig. 1, a part of the packet data inputted by the input and output terminal 108 is inputted into the control circuit 104 via the input and output circuit 107 at the time of recording. In the control circuit 104, the type of packet data and the like is detected by information attached to the packet data or information that has been sent separately to the packet data, the recording mode is determined by the detection result, and the operation modes of the recording signal processing circuit 102a and the servo circuit 106 are set. The input and output circuit

**THIS PAGE BLANK (USPTO)**

107 then outputs to the data encryption circuit 115 the packet data to be recorded. In the data encryption circuit 115, by generation of the data key in the control circuit 104 based on the key to be generated by the device key generator 117 and the block key generator 118, the packet data is encrypted and the encrypted packet data is outputted to the input and output control circuit 119. In the input and output control circuit 119, based on the timing information from the timing generation circuit 105, the time stamp is given to the inputted packet data and the inputted packet data given the time stamp is outputted to the recording signal processing circuit 102a. In the recording signal processing circuit 102a, according to the recording mode determined by the control circuit 104, the generation of recording data such as the error correction decryption, the ID information, the sub-code, the block key information used in encryption, and the like is performed and the recording signal is generated, which is recorded onto the tape 111 by the rotating head 100.

20 [0017] At the time of reproduction, a reproduction operation is firstly performed in an optional reproducing mode and the ID information is detected by the reproduction signal processing circuit 102b. It is determined by the control circuit 104 as to what mode recording has been performed in and reproduction is performed by resetting the operation modes of the reproduction signal processing circuit 102b and the servo circuit 106. In the reproduction signal processing circuit 102b, the detection of the synchronization signal, the correction of error detection, and the acquisition of block key information or the like are performed from the reproduction signal reproduced by the rotating head 100 and the packet data is outputted to the input and output control circuit 119 after

**THIS PAGE BLANK (USPTO)**



being reproduced. In the input and output control circuit 119, the packet data free of the time stamp is outputted to the data decryption circuit 116 as the reference of the timing generated by the timing generation circuit 105. In the data decryption circuit 116, based on the key generated by the device key generator 117 and the block key obtained by the reproduction, the packet data free of the time stamp is decrypted by the data key generated in the control circuit 104 and outputted to the input and output circuit 107.

[0018] At the time of recording, the operation timing of the recording and reproducing apparatus is controlled by the timing control circuit 109 as the reference of the rate of recording data inputted by the input and output terminal 108. At the time of reproduction, an oscillated clock is operated by the oscillating circuit 110 as the reference of the operation.

[0019] Fig. 3 is a configuration diagram of the packet of the digital video compressed signal. One packet is constituted of a fixed length, for example, 188 bytes, and includes a 4-byte packet header 306 and 184-byte packet information 307. The digital compressed video signal is positioned in the region of the packet information 307. The packet header 307 is constituted of information such as the type of packet information.

[0020] Fig. 4 is a configuration diagram of the packet header 306 in Fig. 3. 501 is a synchronization byte indicating the head of the packet, 502 is an error display indicating presence of an error, 503 is a unit start display indicating a start of a unit, 504 is packet priority indicating the importance of the packet, 505 is a packet ID indicating the type of a packet, 506 is scrambling control indicating the presence of scrambling,

**THIS PAGE BLANK (USPTO)**

507 is adaptation field control indicating presence of additional information and presence of packet information, and 508 is a checking counter for counting up in packet units.

5 [0021] Fig. 5 is a configuration diagram of transmitted signals of the digital broadcast and the signals selected from the transmitted signals. 71 is a packet in Fig. 3. Normally, the sound signal, information relating to a program, and the like are attached to the video signal  
10 mentioned above. Programs of multiple channels are transmitted by time-division multiplexing.

[0022] Fig. 5(a) is an example of a multiplexed three channel program. V1, V2, and V3 are video signals for the respective channels and A1, A2, A3 are packets of the sound  
15 signals for the respective channels. A single channel can be constituted of multiple videos and sounds. P0, P1, P2, and P3 are information relating to the programs. A different packet ID 505 is allocated to each packet. Thus, identification of packet's contents can be done.

20 [0023] P0 is information relating to the whole of the transmitted signal in Fig. 5(a). Packets such as the program association table for identifying as to what packet ID is allocated to each program and the program guide information are transmitted by time-division multiplexing.  
25 P1, P2, and P3 are information relating to the respective programs. Packets such as a program map table for identifying which packet IDs have been allocated to the video packet, the sound packet, and the like of the channels and scrambling information are transmitted by  
30 time-division multiplexing. Normally, a determined value, for example, 0, is allocated to the packet ID of the program association table.

[0024] At the time of reception, it is firstly

**THIS PAGE BLANK (USPTO)**

recognized by the program association table as to what packet ID has been allocated in the program map table for the program desired to be received. It is then recognized by the program map table of the program desired to be  
5 received as to what packet IDs have been allocated to the video packet, the sound packet, and the like. Decryption of the digital compressed data is performed by extracting the video packet and the sound packet. The program clock reference is extracted at the same time. Thus, the  
10 operation of the decryption circuit is controlled so that the decryption timing of the decryption circuit of the digital compressed data is in synchronization with the time of encryption.

[0025] CR is program clock reference information in  
15 order to be in synchronization with the time of decrypting the digital compressed data.

[0026] Of course, the number of channels to be multiplexed can be other than three channels, for example, four channels. Other pieces of information can also be  
20 multiplexed.

[0027] Fig. 5(b) is only the information selected from the first channel from Fig. 5(a) and program information relating thereto. When the first channel is recorded, this information is outputted to the recording and reproducing  
25 apparatus 200 from the digital broadcast receiver 201.

Information other than this can be recorded. In order to facilitate processing at the time of reproduction, a part of the packet information can be changed. For example, if the packet information is changed to only information of  
30 the program for recording program association table information, channel selection is unnecessary at the time of reproduction.

[0028] Fig. 6 is a configuration diagram of the data

**THIS PAGE BLANK (USPTO)**

encryption circuit 115 in Fig. 2. 1151 is a packet data input terminal, 1157 is a packet data output terminal, 1153a and 1153b are data key input terminals, 1153c is a data key selection signal input terminal, 1153d is a  
5 processing mode selection signal input terminal, 1152 and 1156 are block processing circuits, 1154 is a key schedule circuit, 1155 is an encryption device, 1158a and 1158b are data key registers, and 1159 is a data key selector. The data encryption circuit 115 outputs by encrypting inputted  
10 packet data units by a data key determined in advance. The stability of the packet data being recorded onto a tape can be increased by the data key being changed at a certain time interval.

[0029] In the encryption device 1155, for example, even  
15 if an error such as a bit error occurs during transmission, the error has no influence on the following data. In other words, so there is no error propagation, a block encryption that can realize encryption processing by a simple circuit configuration for a block constituted of multiple bits is  
20 used by the encryption device 1155.

[0030] The packet data inputted from the input terminal 115 is firstly segmented into block P including multiple bits in the block processing circuit 1152. For example, one block is 64 bits. Each block is sequentially encrypted  
25 in the encryption device 1155. The block C is thus outputted and in the block processing circuit 1156, the block is returned to the form of packet data and outputted to the output terminal 1157. The data key, which is the key for encryption, is inputted from the data key input  
30 terminals 1153a and 1153b by the control circuit 104 and stored in the data key registers 1158a and 1158b. For example, the present data key is recorded in the data key register 1158a and the data key to be switched to next is

**THIS PAGE BLANK (USPTO)**



recorded in the data key register 1158b.

[0031] The signal for indicating which of either the data key register 1158a or 1158b is to be selected is inputted by the control circuit 104 and the selected data key is outputted by the data key selector 1159 from the data key selection signal input terminal 1153c. For example, the data key of the key register 1158a is selected. The selected data key is changed to sub keys KA and KB in the scheduling circuit 1154 and supplied to the encryption device 1155. For example, the length of the data key is 56 bits and the length of each sub keys is 32 bits. The top 32 bits of the data key are allocated to KA and the additional value of the top 32 bits and the bottom 32 bits of the data key are allocated to KB.

[0032] When the data key is changed, a signal is inputted from the data key selection signal input terminal 1153c by the control circuit 104 so that the data key register 1158b will output. The data key selector does not switch the selected output until the encryption of the blocks for one packet data has completely finished and is controlled so as to switch between packet data.

**THIS PAGE BLANK (USPTO)**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-293936

(P2000-293936A)

(43) 公開日 平成12年10月20日 (2000. 10. 20)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 1 1 B 20/10	3 0 1	G 1 1 B 20/10	H 5 C 0 5 3
	1 0 2		3 0 1 Z 5 D 0 4 4
20/12		20/12	1 0 2
H 0 4 N 5/91		H 0 4 N 5/91	P
5/92		5/92	H
審査請求 未請求 請求項の数28 O L (全 28 頁)			

(21) 出願番号 特願平11-100976

(22) 出願日 平成11年4月8日 (1999. 4. 8)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 佐々本 学

神奈川県横浜市戸塚区吉田町292番地株式

会社日立製作所マルチメディアシステム開  
発本部内

(72) 発明者 岡本 宏夫

神奈川県横浜市戸塚区吉田町292番地株式

会社日立製作所マルチメディアシステム開  
発本部内

(74) 代理人 100075096

弁理士 作田 康夫

最終頁に続く

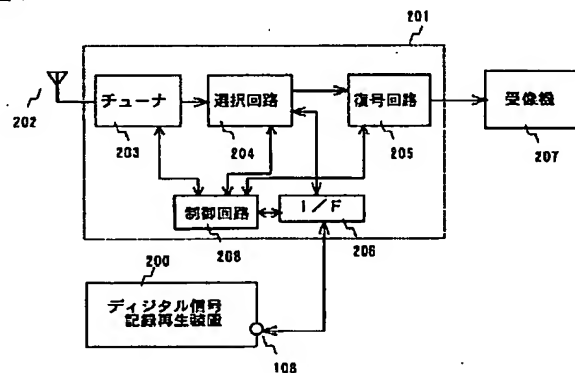
(54) 【発明の名称】 デジタル信号記録装置、再生装置、および記録媒体

(57) 【要約】

【課題】 記録媒体上のデジタル信号の著作権を保護できる記録装置、再生装置、および記録媒体を提供することにある。

【解決手段】 デジタル信号を、記録媒体上に記録または再生するデジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力することにより達成できる。

図 1



## 【特許請求の範囲】

【請求項 1】 デジタル信号を記録媒体上に記録するデジタル信号記録装置において、

少なくとも一つの鍵情報を発生する鍵情報発生手段と、前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記デジタル信号が入力され、前記鍵で前記デジタル信号を暗号化して出力する暗号変換手段と、少なくとも一つの前記鍵情報を、暗号化された前記デジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするデジタル信号記録装置。

【請求項 2】 前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項 1 記載のデジタル信号記録装置。

【請求項 3】 前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を備え、前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記記録媒体上の所定の領域に記録する機能を備えたことを特徴とする請求項 1 記載のデジタル信号記録装置。

【請求項 4】 前記デジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記デジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項 3 記載のデジタル信号記録装置。

【請求項 5】 前記暗号変換手段は、さらに、前記デジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を備え、前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求項 1 記載のデジタル信号記録装置。

【請求項 6】 前記デジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を、前記デジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求項 5 記載のデジタル信号記録装置。

【請求項 7】 所定長のデジタル信号を入力して、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第 1 の誤り訂正符号を付加し、さらに  $n$  ( $n$  は 1 以上の整数) セクタ単位で第 2 の誤り訂正符号を付加し、前記第 2 の誤り訂正符号にも第 1 の誤り訂正符号を付加して記録媒体上に記録するデジタル信号記録装置において、

少なくとも一つの鍵情報を発生する鍵情報発生手段と、前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記デジタル信号が入力され、前記鍵で前記デジタル信号を暗号化して出力する暗号変換手段と、少なくとも一つの前記鍵情報を、暗号化された前記デジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを備えたことを特徴とするデジタル信号記録装置。

10 【請求項 8】 前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を有し、前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、前記所定の演算を行って更新された鍵を発生し、

前記暗号変換手段は、前記第 2 の誤り訂正符号を付加した  $n$  セクタの単位の区切り目で、前記更新された鍵に切り換える機能を備えたことを特徴とする請求項 7 記載のデジタル信号記録装置。

20 【請求項 9】 前記暗号変換手段は、前記デジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を有し、

前記記録手段は、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、

前記第 2 の誤り訂正符号を付加したセクタの単位の区切り目で、前記デジタル信号を暗号化するか否かを切り換える機能を備えたことを特徴とする請求項 7 記載のデジタル信号記録装置。

30 【請求項 10】 記録媒体上に記録されているデジタル信号を再生するデジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記デジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と再生された前記デジタル信号が入力され、前記鍵で前記デジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするデジタル信号再生装置。

40 【請求項 11】 前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項 10 記載のデジタル信号再生装置。

【請求項 12】 少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力されて所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項 10 記載のデジタル信号再生装置。

50 【請求項 13】 前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情

報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求項 10 記載のデジタル信号再生装置。

【請求項 14】前記デジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記デジタル信号の各パケットに付加して記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求項 13 記載のデジタル信号再生装置。

【請求項 15】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を、再生する機能を備え、

前記復号変換手段は、前記暗号フラグ情報により、再生された前記デジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項 10 記載のデジタル信号再生装置。

【請求項 16】前記デジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記デジタル信号の各パケットに付加されて記録されているところの、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求項 15 記載のデジタル信号再生装置。

【請求項 17】所定長のデジタル信号に、同期信号、管理情報信号を付加してセクタ形式とし、前記セクタに第 1 の誤り訂正符号を付加し、さらに  $n$  ( $n$  は 1 以上の整数) セクタ単位で第 2 の誤り訂正符号を付加し、前記第 2 の誤り訂正符号にも第 1 の誤り訂正符号を付加して、記録媒体上に記録されている前記デジタル信号を再生するデジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記デジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と再生された前記デジタル信号が入力され、前記鍵で前記デジタル信号を復号化して出力する復号変換手段とを備えたことを特徴とするデジタル信号再生装置。

【請求項 18】少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが

入力され、所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求項 17 記載のデジタル信号再生装置。

【請求項 19】前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報を、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記更新された鍵に切り換える手段を備えたことを特徴とする請求項 17 記載のデジタル信号再生装置。

【請求項 20】前記再生手段は、前記第 2 の誤り訂正符号を付加した  $n$  セクタの単位の区切り目で更新されているところの、前記鍵情報を、再生していく機能を備えたことを特徴とする請求項 19 記載のデジタル信号再生装置。

【請求項 21】前記再生手段は、前記記録媒体上の所定の領域に記録されている、前記デジタル信号が暗号化されているか否かを示す暗号フラグ情報を再生する機能を備え、前記復号変換手段は、前記暗号フラグ情報により、再生された前記デジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求項 17 記載のデジタル信号再生装置。

【請求項 22】前記再生手段は、前記第 2 の誤り訂正符号を付加した  $n$  セクタの単位の区切り目で切り換えられているところの、前記暗号フラグを、再生していく機能を備えたことを特徴とする請求項 21 記載のデジタル信号再生装置。

【請求項 23】デジタル信号が記録されているデジタル信号記録媒体において、鍵情報に所定の演算を行って得られた鍵で暗号化された前記デジタル信号と共に、前記鍵情報が、所定の領域に記録されていることを特徴とするデジタル信号記録媒体。

【請求項 24】前記デジタル信号は、所定長のパケット形式を有してなることを特徴とする請求項 23 記載のデジタル信号記録媒体。

【請求項 25】前記鍵情報が所定間隔で更新され、所定の領域に記録されていることを特徴とする請求項 23 記載のデジタル信号記録媒体。

【請求項 26】デジタル信号を変換するための複数種類の鍵を発生する鍵発生手段と、前記鍵を用いてデジタル信号を変換し、変換後の変換デジタル信号を出力する変換手段と、前記鍵および前記変換デジタル信号を記録媒体に記録する記録手段と、

を備えてなることを特徴とするデジタル信号記録装置。

【請求項 27】複数種類の鍵で変換された変換デジタル信号および前記鍵が記録された媒体が用いられ、前記変換デジタル信号および前記鍵を前記媒体から再生し、出力する再生手段と、

前記再生手段からの出力が入力され、前記変換デジタル信号を前記鍵を用いて復号変換する復号変換手段と、を備えてなるデジタル信号再生装置

【請求項 28】複数種類の鍵で変換された変換デジタル信号および前記鍵が記録された記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル信号を記録媒体に記録再生するデジタル信号記録装置、再生装置、および記録媒体に関し、特に記録媒体上のデジタル信号の著作権を保護する機能を有するデジタル信号記録装置、再生装置、および記録媒体に関する。

【0002】

【従来の技術】近年、デジタル技術を用いた映像、音声等のデータ圧縮の研究が進み、これらデータの蓄積、伝送が容易にできるようになった。これに伴い、放送の分野においてもデジタル化が急速に進められている。

【0003】例えば、アナログ映像信号、音声信号を MPEG (Moving Picture Experts Group) 規格を用いて高能率にデジタル圧縮符号化し、衛星や同軸ケーブルを通して放送するシステムが知られている。このデジタル放送を受信するための装置として、セットトップボックスと呼ばれるデジタル放送受信機がある。

【0004】また、家庭用の映像信号、音声信号記録再生機器としては、磁気テープを用い、デジタルTV放送などのデジタル圧縮符号化された映像信号及び音声信号をデジタル信号のまま記録し再生できるデジタルVTRの開発が進められている。

【0005】このデジタル放送受信機とデジタルVTRは、デジタルインターフェースで接続され、受信したデジタル放送を高品質で保存可能となる。

【0006】さらに、光ディスクやハードディスクを用い、映像信号及び音声信号を記録し再生する装置の開発が進められている。

【0007】複数の情報が多重されて伝送されてくるデジタル信号を受信して所望の番組を選択する技術が、日本特開平8-56350号に述べられている。また、回転磁気ヘッドを用いたデジタルVTRについては、例えば、日本特開平5-174496号に記載されている。

【0008】さらに、デジタル放送受信機とデジタルVTRをデジタルインターフェースで接続したデジタル放送記録システムについて、アイイーイーイー トランザクションズ オン コンシューマー エレクトロニクス、第42巻3号、1996年8月、617~622頁 (IEEE Transactions on Consumer Electronics、

Vol. 42, No. 3, August 1996, p617~622 「Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era」) に詳しく述べている。

【0009】

【発明が解決しようとする課題】しかしながら、デジタル放送等をデジタルVTR等で記録した、記録媒体上のデジタル信号の著作権の防衛については何ら考慮されていない。

【0010】本発明の目的は、記録媒体上のデジタル信号の著作権を保護することにある。

【0011】

【課題を解決するための手段】本発明は、デジタル信号を、記録媒体上に記録または再生するデジタル信号記録装置、再生装置および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力する。

【0012】

【発明の実施の形態】以下、本発明の実施例を図面を用いて説明する。

【0013】図1はデジタル放送受信機とデジタル信号記録再生装置を含む構成図である。200はデジタル信号記録再生装置、201はデジタル放送受信装置、202はアンテナ、207は受像機である。また、203はチューナ、204は選択回路、205は復号回路、206はインターフェース回路、208はデジタル放送受信機201の動作の制御を行う制御回路である。ここで、デジタル放送受信機201とデジタル信号記録再生装置200は別体の構成で表示されているが、一体の構成となってもよい。

【0014】図2は図1のデジタル信号記録再生装置200の構成図である。図2は記録再生兼用の装置であるが、記録と再生が独立していても同様である。100は回転ヘッド、101はキャプスタン、102aは記録時の記録信号の生成等を行う記録信号処理回路、102bは再生時の再生信号の復調等を行う再生信号処理回路、104は記録再生モード等の制御を行う、例えば、マイクロプロセッサのような制御回路、105は回転ヘッド100の回転等の基準となるタイミング信号を生成するタイミング生成回路、106は回転ヘッド及びテープの送り速度を制御するサーボ回路、107は記録信号の入力または再生信号の出力を行う入出力回路、109は記録時のタイミングを制御するタイミング制御回路、110は基準クロックを生成する発振回路、111はテープ、112はアナログ映像信号の記録再生回路、115はデジタル信号記録時のデータ暗号回路、116はデジタル信号再生時のデータ復号回路、117は、デジタル情報を暗号あるいは復号する際にデータ暗号回

7  
路 115 あるいはデータ復号回路 116 に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、118 はデジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるブロック鍵を発生するブロック鍵発生器、119 は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

【0015】デジタル映像圧縮信号は、パケット形式のデータで、複数チャンネルの信号が時分割多重されて伝送される。図 1 において、アンテナ 202 で受信されたデジタル放送信号は、チューナ 203 で復調され、その後、選択回路 204 で必要なデジタル圧縮映像信号が選択される。選択されたデジタル圧縮映像信号は、復号回路 205 で通常の映像信号に復号されて、受像機 207 に出力される。また、受信信号にスクランブル等の処理が行われているときは、選択回路 204 においてそれを解除した後に、復号処理が行なわれる。受信したデジタル放送信号の記録を行うときは、選択回路 204 において記録するデジタル圧縮映像信号及びそれに関連した情報が選択され、インターフェース回路 206 を介してデジタル信号記録再生装置 200 の入出力端子 108 より、デジタル信号記録装置 200 に入力され、記録される。また、記録したデジタル放送信号の再生を行うときは、デジタル信号記録再生装置 200 で再生されたデジタル圧縮映像信号等が、入出力端子 108 よりインターフェース回路 206 に出力される。インターフェース回路 206 に入力されたデジタル圧縮映像信号等は、選択回路 204、復号回路 205 により、通常の受信時と同様の処理を行って、受像機 207 に出力する。

【0016】図 1 のデジタル信号記録再生装置 200 の構成を示す図 2 において、記録時には、入出力端子 108 より入力されたパケットデータの一部分が、入出力回路 107 を介して制御回路 104 に入力される。制御回路 104 では、パケットデータに付加されている情報あるいはパケットデータとは別に送られてきた情報によりパケットデータの種類等を検出し、検出結果によって記録モードを判断し、記録信号処理回路 102a 及びサーボ回路 106 の動作モードを設定する。次に入出力回路 107 は、記録するパケットデータをデータ暗号回路 115 に出力する。データ暗号回路 115 では、デバイス鍵発生器 117 およびブロック鍵発生器 118 により発生される鍵をもとに制御回路 104 において生成されるデータ鍵によって、入力されたパケットデータを暗号化し、これを入出力制御回路 119 に出力する。入出力制御回路 119 では、タイミング生成回路 105 からの時間情報をもとに、入力されたパケットデータにタイムスタンプを施し、これを記録信号処理回路 102a に出力する。記録信号処理回路 102a では、制御回路 104 で判断された記録モードに応じて、誤り訂正符号、ID

情報、サブコード、暗号化に使用したブロック鍵情報等を含む記録データの生成を行い且つ記録信号を生成して、回転ヘッド 100 によりテープ 111 に記録する。

【0017】再生時には、まず任意の再生モードで再生動作を行い、再生信号処理回路 102b で ID 情報を検出する。そして、制御回路 104 でどのモードで記録されたかを判断し、再生信号処理回路 102b 及びサーボ回路 106 の動作モードを再設定して再生を行う。再生信号処理回路 102b では、回転ヘッド 100 より再生された再生信号より、同期信号の検出、誤り検出訂正、ブロック鍵情報等の取得を行い、パケットデータを再生して入出力制御回路 119 に出力する。入出力制御回路 119 では、タイミング生成回路 105 で生成されたタイミングを基準としてタイムスタンプを取り除いたパケットデータをデータ復号回路 116 に出力する。データ復号回路 116 では、デバイス鍵発生器 117 により発生される鍵、および再生によって得られたブロック鍵をもとに、制御回路 104 において生成されるデータ鍵によって復号して、入出力回路 107 に出力する。

【0018】記録時には、入出力端子 108 より入力された記録データのレートを基準としてタイミング制御回路 109 により記録再生装置の動作タイミングを制御し、再生時には、発振回路 110 により発振されたクロックを動作基準として動作する。

【0019】図 3 はデジタル映像圧縮信号のパケットの構成図である。1 パケットは固定長、例えば、188 バイトで構成されており、4 バイトのパケットヘッダ 306 と、184 バイトのパケット情報 307 により構成されている。デジタル圧縮映像信号は、パケット情報 307 の領域に配置される。また、パケットヘッダ 307 はパケット情報の種類等の情報により構成される。

【0020】図 4 は図 3 のパケットヘッダ 306 の構成図である。501 はパケットの先頭を示す同期バイト、502 は誤りの有無を示す誤り表示、503 はユニットの開始を示すユニット開始表示、504 はパケットの重要度を示すパケットプライオリティ、505 はパケットの種類を示すパケット ID、506 はスクランブルの有無を示すスクランブル制御、507 は追加情報の有無及びパケット情報の有無を示すアダプテーションフィールド制御、508 はパケット単位でカウントアップされる巡回カウンタである。

【0021】図 5 はデジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。71 は図 3 のパケットである。通常、上記映像信号に音声信号、プログラムに関する情報等が付加され、複数チャンネルのプログラムが時分割多重されて伝送される。

【0022】図 5 (a) は、3 チャンネルのプログラムを多重した例であり、V1、V2、V3 はそれぞれのチャンネルの映像信号、A1、A2、A3 はそれぞれのチャンネルの音声信号のパケットである。なお、映像また

は音声は、一つのチャンネルに複数の映像または音声で構成されている場合もある。P0、P1、P2、P3はプログラムに関する情報である。それぞれのパケットは、異なるパケットID505が割り当てられており、これによりパケットの内容を識別することができる。

【0023】P0は、図5(a)の伝送信号全体に関する情報であり、それぞれのプログラムにどのパケットIDが割り当てられているかを認識するためのプログラムアソシエーションテーブル、番組ガイド情報等のパケットが時分割多重されて伝送される。P1、P2、P3は、それぞれのプログラムに関する情報であり、そのチャンネルの映像パケット、音声パケット等にどのパケットIDが割り当てられているかを認識するためのプログラムマップテーブル、スクランブル情報等のパケットが時分割多重されて伝送される。通常、プログラムアソシエーションテーブルのパケットIDは決まった値、例えば0が割り当てられている。

【0024】受信時には、まずプログラムアソシエーションテーブルによって受信したいプログラムのプログラムマップテーブルにどのパケットIDが割り当てられているかを認識し、次に、受信したいプログラムのプログラムマップテーブルによって映像パケット、音声パケット等にどのパケットIDが割り当てられているかを認識する。そして、映像パケットおよび音声パケットを抽出してディジタル圧縮データの復号を行う。また、同時にプログラムクロックリファレンスを抽出し、これによってディジタル圧縮データの復号回路の復号タイミングが符号化時のタイミングと同期するように復号回路の動作を制御する。

【0025】CRは、ディジタル圧縮データの復号時の同期をとるためのプログラムクロックリファレンス情報である。

【0026】もちろん、多重するチャンネル数は3チャンネル以外、例えば4チャンネルでもよいし、また、これ以外の情報を多重してもよい。

【0027】図5(b)は、図5(a)から第1のチャンネルの情報およびそれに関連したプログラム情報のみを選択したものである。第1のチャンネルを記録する場合には、この情報をディジタル放送受信機201から記録再生装置200に出力する。もちろん、これ以外の情報を含めて記録してもよいし、また、再生時の処理をやりやすくするために、パケットの情報の一部を変更してもよい。例えば、プログラムアソシエーションテーブルの情報を記録するプログラムのみの情報に変更すれば、再生時にチャンネルの選択が不要になる。

【0028】図6は図2のデータ暗号回路115の構成図である。1151はパケットデータ入力端子、1157はパケットデータ出力端子、1153a、1153bはデータ鍵入力端子、1153cはデータ鍵選択信号入力端子、1153dは、処理モード選択信号入力端子、

1152、1156はブロック処理回路、1154は鍵スケジュール回路、1155は暗号器、1158a、1158bはデータ鍵レジスタ、1159はデータ鍵セクタである。データ暗号回路115は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で暗号化して出力する。この際、このデータ鍵をある時間間隔で変更していくことにより、テープ上に記録されるパケットデータの安全性を高めることができる。

【0029】暗号器1155は、例えば、伝送中にビット誤り等のエラーが発生しても、そのエラーが後続のデータに影響を与えない、すなわちエラー伝播がないように、複数ビットで構成されるブロックを単位として暗号処理を簡単な回路構成で実現できるブロック暗号を用いる。

【0030】入力端子1151から入力されたパケットデータは、まず、ブロック処理回路1152において、複数ビットからなるブロックPに区切られる。例えば1ブロックを64ビットとする。各ブロックは、暗号器1155において順次暗号化され、その結果ブロックCを出力し、ブロック処理回路1156において、今度はブロックをパケットデータの形式に戻して出力端子1157へ出力する。ここで、暗号化のための鍵であるデータ鍵は、制御回路104より、データ鍵入力端子1153aおよび1153bから入力され、データ鍵レジスタ1158a、1158bに記憶される。例えば、データ鍵レジスタ1158aには、現在のデータ鍵を、データ鍵レジスタ1158bには次に切り換えるデータ鍵を記録させる。

【0031】また、データ鍵選択信号入力端子1153cからは、制御回路104より、データ鍵レジスタ1158a、1158bのどちらのデータ鍵を選択するかを示す信号が入力され、データ鍵セクタ1159により、選択されたデータ鍵が出力される。ここでは、例えば鍵レジスタ1158aのデータ鍵が選択されているものとする。選択されたデータ鍵は、スケジュール回路1154においてサブ鍵KA、KBに変換され、暗号器1155に供給される。例えば、データ鍵の長さ56ビット、サブ鍵の長さが、それぞれ32ビットとし、データ鍵の上位32ビットをKAに割り当て、データ鍵の上位32ビットと下位32ビットの加算値をKBに割り当てる。

【0032】ここで、データ鍵を変更する場合には、制御回路104より、データ鍵レジスタ1158bを出力するようデータ鍵選択信号入力端子1153cから信号が入力される。データ鍵セクタは、一つのパケットデータのブロック全ての暗号化が終了するまでは、その選択出力を切り換えず、次のパケットデータとの間で切り換えるよう制御する。

【0033】その他、例えば、暗号器1155の出力と、暗号器1155の入力を排他的論理和をとり、プロ



ック単位でフィードバックをかけることで、暗号強度を増す方法もある。

【0034】図7は図6の暗号器1155の構成図である。同図中、551、552、553、554は暗号処理部、Pa、Pbは入力ブロックデータPの上位および下位ビット、Ca、Cbは暗号化されたデータ、KA、KBは、サブ鍵である。同図に示すように、例えば入力された64ビットのブロックPを、その上位32ビットPaと下位32ビットPbに分離する。そのPa、Pbは、暗号処理部551において、排他的論理和(5511)、ビットシフトおよび加算演算(5512、5513、5515:  $A << p$  は、Aをpビット左方向に循環ビットシフトすることを表す)、加算演算(5514、5516)を行い、その結果を暗号処理部551と同様の処理を行う後続の暗号処理部552、553、さらに図示しない暗号処理部に入力して複数段繰り返し演算を行い、最終段の暗号処理部554により出力されたデータCa、Cbより、暗号化されたブロックCを得る。

【0035】以上は、図2、図7のデータ暗号回路115について説明したが、図2のデータ復号回路116では、暗号器1155の逆の流れで演算していくことにより、暗号化されたブロックを復号することができる。ただし、図7の演算5516は、減算処理とする。また、当然、サブ鍵KA、KBは、暗号時と同一の鍵を用いなければならない。

【0036】その他、記録するパケットデータを保護する必要が無い場合、例えば記録する番組が自由にコピーしてもよいよう許可されている場合、パケットデータを暗号化しないで、そのままテープ上に記録する場合がある。これは例えば、データ暗号回路115、データ復号回路116を、入力パケットの暗号・復号の機能と、なにもしないで通過させる機能とを切り換えることで実現できる。図2、図6のデータ暗号回路115において、図6の処理モード選択信号入力端子1153dを介して入力される処理モード選択信号により、図7の演算5516への入力X5を、図示していないが、零に固定することで、暗号、復号処理を行わずに、ブロックを通過させることが出来る。この方法によれば、入力パケットの通過遅延時間を一定に保ったまま、動作を切り換えることができる。また、図示しないが、他の方法としては、入力端子1151から入力されたパケットデータを、ブロック処理回路1152、暗号器1155、ブロック処理回路1156を介さず、出力端子1157に出力するか、ブロック処理回路1156から出力されるパケットデータを出力端子1157に出力するかを切り換える切り換え回路を出力端子1157の前段に設け、処理モード選択信号入力端子1153dを介して入力される処理モード選択信号をその切り換え回路に入力して、ブロック処理回路1156から出力されるパケットデータか、

入力端子1157に入力されたパケットデータかを切り換える方法もある。これらの方法は、図2、図19のデータ復号回路116においても前述と同様の構成で実現できる。

【0037】図8は図2のデータ暗号回路115、データ復号回路116に供給するデータ鍵の生成例を示すところの制御回路104内のデータ鍵の生成図である。デバイス鍵発生器117は、例えば96ビットのあらかじめ定められた固定の鍵情報を記憶している。ブロック鍵発生器118は、例えば図2の制御回路104からの司令1181により、96ビットの乱数を発生させる乱数発生器である。120は96ビットの排他的論理和演算器、121はハッシュ関数演算器である。図8(a)では、ブロック鍵とデバイス鍵は、排他的論理和演算器120で排他的論理和がとられ、ハッシュ関数演算器121にてハッシュ演算がなされ、その結果のうちの選択された56ビットが、データ鍵として図2のデータ暗号回路115に供給される。ハッシュ関数は、その出力結果から、入力データが類推困難な関数であり、データ鍵から、秘密情報であるブロック鍵、デバイス鍵が求められない。

【0038】また、図2の制御回路104からの司令1181をある時間間隔で発生させ、上述の演算によるデータ鍵生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、記録媒体上のデータの安全性を高めることが可能となる。次に、ブロック鍵発生器118で発生されたブロック鍵(Kr)は、図2の記録信号処理回路102aに送られ、テープ111上に記録される。

【0039】再生時には、ブロック鍵発生器118の発生するブロック鍵の代わりに、テープ111上から再生されたブロック鍵(Kp)を用いて、上記と同様の演算を行い、データ鍵を得、図2のデータ復号回路116に供給される。

【0040】図8(b)は、テープ111上に記録する鍵情報Krとして、ブロック鍵をデバイス鍵で排他的論理和演算したものを用いる例である。この場合、ハッシュ関数演算器にはブロック鍵そのものが入力される。再生時には、図8(a)中のブロック鍵の代わりに、テープ111上から再生されたKpを用いて、上記と同様の演算を行い、データ鍵を得、データ復号回路116に供給される。

【0041】次に、テープへの記録方法について述べる。

【0042】図9は、1トラックの記録パターンである。3は時間情報、プログラム情報等のサブコードを記録するサブコード記録領域、7はディジタル圧縮映像信号を記録するデータ記録領域、2及び6はそれぞれの記録領域のプリアンブル、4及び8はそれぞれの記録領域のポストアンブル、5はそれぞれの記録領域の間のギャ

ップ、1及び9はトラック端のマージンである。このように、各記録領域にポストアンプ、プリアンプ及びギャップを設けておくことにより、それぞれの領域を独立にアフレコを行うことができる。もちろん、記録領域7にはデジタル圧縮映像信号以外のデジタル信号を記録してもよい。データ記録領域7は、複数のブロック（前述の暗号化の小単位であるブロックとは異なる）により構成されている。

【0043】図10は図9のデータ記録領域7のブロックの構成図である。20は同期信号、21はID情報、22はデータ、23は第1の誤り検出訂正のためのパリティ（C1パリティ）である。例えば、同期信号20は2バイト、ID情報21は3バイト、データ22は99バイト、パリティ23は8バイトで構成されており、1ブロックは112バイトで構成されている。

【0044】図11は図10のID情報21の構成図である。31はグループ番号、32はトラックアドレス、33は1トラック内のブロックアドレス、35はグループ番号31、トラックアドレス32及びブロックアドレス33の誤りを検出するためのパリティである。ブロックアドレス33は、各記録領域でのブロックの識別を行うためのアドレスである。例えば、図9のデータ記録領域7では0～335とする。トラックアドレス32は、トラックの識別を行うためのアドレスであり、例えば、1トラックまたは2トラック単位でアドレスを変化させ、nトラックを識別することが出来る。例えば、0～5または0～2とすることにより、6トラックを識別することができる。図11のグループ番号31は、例えば、トラックアドレス32で識別する6トラック単位で変化させ、0～15とすることにより、96トラックを識別することができる。トラックアドレス32は、後述する第2の誤り訂正符号の周期と同期させておけば、記録時の処理及び再生時の識別を容易にすることができる。

【0045】図12は図9のデータ記録領域7の1トラック分のデータの構成図である。なお、図10に図示の同期信号20およびID情報21は省略してある。データ記録領域7は、例えば、336ブロックで構成されており、最初の306ブロックにデータ41を、次の30ブロックに第2の誤り訂正符号（C2パリティ）43を記録する。C2パリティ43は、nトラック単位、例えば6トラック単位で構成されている。6トラック単位でみると、データは306ブロック×6トラックのデータであり、そのデータを18分割して、それぞれの102ブロックに、10ブロックのC2パリティを付加する。誤り訂正符号は、例えばリードソロモン符号を用いればよい。各ブロック99バイトのデータは、3バイトのヘッダ44と96バイトのデータ41により構成されている。

【0046】図13は、188バイトのパケット形式で

伝送されたデジタル圧縮映像信号を、図12のデータ41に記録する時の1パケットのブロックの構成例である。この場合には、4バイトの時間情報25を付加して192バイトとし、2ブロックに1パケットを記録する。時間情報25は、パケットの伝送された時間の情報である。すなわち、パケットの先頭が伝送された時の時間またはパケット間の間隔を基準クロックでカウントし、そのカウント値をパケットデータと共に記録しておき、再生時にその情報を基にしてパケット間の間隔を設定することにより、伝送された時と同一の形でデータを出力することができる。

【0047】図14は図12のデータ記録領域7のヘッダ44の構成図である。ヘッダ44は、フォーマット情報45、ブロック情報46および付加情報47により構成される。フォーマット情報45、およびブロック情報46には、記録に関する様々な記録情報が、また付加情報47には、その他補助的な情報が記録される。

【0048】フォーマット情報45は、記録フォーマットに関する情報であり、記録モード（標準速モードその他の識別）、取り扱うパケットデータの種類、記録されているパケットデータがコピー可能か否か等を示すコピー制限情報等が格納され、複数のブロックで、1つの情報を構成する。例えば12ブロックの12バイトで1つの情報を構成している。そして、この情報を複数回繰り返し多重記録することにより、再生時の検出能力を向上させている。ここに、前述の鍵情報等をも記録しておくことが可能である。

【0049】ブロック情報46は、データ記録領域41に記録されるデータの種別を識別するための情報である。ここには、高速可変速再生用データの有無、種類（どの速度に対応した高速可変速再生用データであるか）等を記録しておく。ここに、前述の鍵情報等をも記録しておくことも可能である。

【0050】付加情報47は、例えば、6ブロックの6バイトで一つの情報であるバックデータを構成し、最初の1バイトが情報の種別を表すアイテムコード、残りの5バイトをデータとすることにより、いろいろな種類のデータを記録することができる。例えばここに前述のブロック鍵等の鍵情報や、その他、記録時間等の情報や記録信号の種類等を記録しておくことができる。

【0051】図15は図14の付加情報47の領域に、ブロック鍵を格納する場合のバックデータの構成図である。

【0052】バックデータの最初の1バイトには後続の情報が鍵情報であることを示すアイテム情報コードを格納する。

【0053】2バイト目には、格納されている鍵の種別を示す情報（鍵シーケンス番号、鍵属性、鍵フラグ）を記録する。前述のように、ブロック鍵をある時間間隔で順次変更していくことで、記録媒体上のデータの安全性

を高めることができるので、例えば、このバックに格納されているブロック鍵が、現在のパケットデータの暗号化に用いられるブロック鍵か、次に用いるブロック鍵かを示す鍵属性情報を記録しておく。また、ブロック鍵が更新される度に反転する鍵フラグで、切り換えタイミングを記録する。この情報により再生時の鍵の切り換えをスムーズにする。また、鍵シーケンス番号には、一つのバックでブロック鍵が格納できない場合、後続のバックがあることを示す情報を格納する。例えばブロック鍵が96ビットの場合、3つのバックに分割して格納し、それぞれの鍵シーケンス番号には、2、1、0を格納し、0が最終バックであることを示す。その他、全体のデータのサイズを格納しておき、残りの大きさを知る方法もある。

【0054】3バイト目から6バイト目に、ブロック鍵を収納する。

【0055】前述の図8(b)の例では、鍵情報K<sub>r</sub>がブロック鍵の代わりに格納される。

【0056】図16はブロック鍵の格納方法を示す図である。この例は、各トラックのバックデータには、現在の鍵情報のみを記録する場合である。したがって、前述の鍵属性は、現在の鍵を示すのみの固定情報であり、記録しなくてもよい。同図中(1)は、96ビットの現在のブロック鍵A(A0乃至A11)が3個のバックに分割して格納される状態を示す。通常、これらのバックは、データの信頼性の向上のため、一つのトラックにつき、複数回記録される。例えば、3個のバックをトラックの最初、半ば、最後のそれぞれの領域に記録する(計9個)ことで、磁気ヘッドの目詰まり等による、再生信号のバースト欠落の影響を軽減できる。また、3個のバックは必ずしも連続したバックとして記録する必要はなく、各バックの間に他の情報を格納したバックを挿入し、鍵情報を格納しているバックを分散して記録することで、鍵情報自身の保護も可能となり、さらに信頼性が向上する。同図(2)はブロック鍵がBに切り換わったトラックに記録されるバックデータである。この場合、ブロック鍵Bの鍵フラグは反転している。

【0057】図17はブロック鍵の他の格納方法を示す図である。図17は、現在の鍵情報と共に、次に使用する鍵情報もあらかじめ発生させておき記録する方法である。ここで、鍵属性情報は、現在のパケットデータの暗号化に用いられるブロック鍵の場合“0”、次に用いるブロック鍵の場合“1”とする。また、ブロック鍵が更新される度に反転する鍵フラグは“0”と“1”を交互に繰り返す。

【0058】同図中(1)は、96ビットの現在のブロック鍵Aが格納される状態を示す。(2)には、次のブロック鍵Bが格納される。この(1)および(2)が、同一のトラック内のブロックの付加情報エリアに記録される。(3)は、ブロック鍵がBに切り換わったトラッ

クに記録されるバックデータである。この場合、ブロック鍵Bは、鍵属性情報“0”の現在の鍵に、また、鍵フラグも反転している。さらに(4)は、次に用いる鍵Cが格納される。(3)および(4)が、同一のトラック内のバックデータとしてトラックに記録される。

【0059】ブロック鍵の更新タイミングを示す鍵フラグの格納場所としては、付加情報47のバックに格納する以外に、前述の図14に示したフォーマット情報45、あるいはブロック情報46に格納する方法もある。

10 【0060】以上のように、鍵情報が、テープ上に記録されるが、ブロック鍵を切り換えるタイミングとしては、前述のC2パリティの付加の単位であるnトラック(本実施例では6トラック)の区切り目とすることで、再生時に、C2パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【0061】また、以上の例ではブロック鍵が更新されるタイミングを示す情報を鍵フラグとして記録したが、図2の記録信号処理回路102aにおいて、前述の図11に示したトラックアドレス32、あるいはグループ番号31の値と、C2パリティの演算の周期および更新のタイミングを同期させることで、特に鍵フラグを記録しなくとも、再生時における鍵情報の更新のタイミングを、このトラックアドレス32あるいはグループ番号31の値で検出することも可能である。例えば、図2の記録信号処理回路102aにおいて、トラックアドレス32が、トラック1本毎に0から5の値を繰り返し、その値0から5の6本のトラックを、前述のC2パリティの付加の単位とする。そして、値が5から0になるタイミングで、データ暗号回路115において、ブロック鍵を更新して、記録する。再生時においては、図2の再生信号処理回路102bにおいて、このトラックアドレス32の値が5から0になるタイミングを検出し、データ復号回路116において、鍵を更新していけばよい。また、さらに長い周期で更新する場合には、例えば、グループ番号31を用いて、トラックアドレス32の値が5から0になる際に、グループ番号31を1増加させ、0から15の値を繰り返すようにすることで、96トラックの単位で、しかもC2パリティの付加の単位の区切り目の、更新のタイミングを検出することが可能となる。

40 【0062】図18は図13の時間情報25(4バイト=32ビット)の具体的構成例であり、鍵フラグ、暗号フラグ格納の他の方法を示したものである。ここでは、例えば、時間情報251としては、22ビットの情報であり、252は前述の鍵フラグ(1ビット)、253は、後続のパケットデータが暗号化されているかどうかを示す暗号フラグ(1ビット)である。記録時には、図2の入出力制御回路119は、タイムスタンプである時間情報251とともに、暗号フラグ253に、後続のパケットデータが暗号化されている場合には例えば“1”を、暗号化されていない場合には“0”を格納し、ま

た、鍵フラグ 252 には、後続のパケットデータに対応する前述の鍵情報を格納するバックデータの鍵フラグを格納する。再生時には、図 2 の入出力制御回路 119 において、記録時に付加した時間情報 25 を取り除いてデータ復号回路 116 に出力するとともに、暗号フラグ 253、鍵フラグ 252 をデータ復号回路 116 に供給し、データ復号回路 116 の動作を制御する。

【0063】図 19 は図 2 のデータ復号回路 116 の構成図である。1161 はパケットデータ入力端子、1167 はパケットデータ出力端子、1163a、1163b はデータ鍵入力端子、1163c はデータ鍵選択信号入力端子、1163d は、処理モード選択信号入力端子、1162、1166 はブロック処理回路、1164 は鍵スケジュール回路、1165 は復号器、1168a、1168b はデータ鍵レジスタ、1169 はデータ鍵セクタである。データ復号回路 116 は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で復号化して出力する。

【0064】復号器 1165 は、複数ビットで構成されるブロックを単位として復号処理を実現するブロック暗号を用いる。

【0065】入力端子 1161 から入力されたパケットデータは、データ暗号回路 115 と同様に、複数ビットからなるブロック C に区切られ、各ブロックは、復号器 1165 において順次復号化され、その結果ブロック P を出力し、ブロック処理回路 1166 において、パケットデータの形式に戻して出力端子 1167 へ出力する。ここで、復号化のための鍵であるデータ鍵は、制御回路 104 より、データ鍵入力端子 1163a および 1163b から入力され、データ鍵レジスタ 1168a、1168b に記憶される。例えば、データ鍵レジスタ 1168a には、現在のデータ鍵を、データ鍵レジスタ 1168b には次に切り換えるデータ鍵を記録させる。

【0066】また、処理モード選択信号入力端子 1163d からは、入出力制御回路 109 より検出した暗号フラグ 253 が入力され、復号器 1165 を復号動作のモードか、何もしないで通過させるモードかを決定する。さらに、データ鍵選択信号入力端子 1163c からは、入出力制御回路 109 より検出した鍵フラグ 252 が入力され、データ鍵セクタ 1169 により、選択されたデータ鍵が出力される。選択されたデータ鍵は、スケジュール回路 1164 においてサブ鍵 KA、KB に変換され、暗号器 1165 に供給される。

【0067】ここで、図 2 の入出力制御回路 119 で検出した、暗号フラグ、あるいは鍵フラグが変化すると、それに連動して、データ復号器 116 の動作モード、データ鍵の選択が行われる。

【0068】以上のように、各パケットデータへ暗号フラグ、鍵フラグを付加することにより、パケットデータ単位での、暗号化の有無、鍵情報の判別、および復号処

理が実現できる。

【0069】その他、暗号化されているかどうかを示す暗号フラグの格納場所としては、図 15 に示した鍵情報を格納するバックの 2 バイト目に格納する方法、あるいは前述の図 14 に示したフォーマット情報 45、ブロック情報 46 に格納する方法もある。

【0070】暗号フラグをフォーマット情報 45、あるいはブロック情報 46 等に格納することで、例えば暗号フラグが“1”を示す時、すなわちパケットデータが暗号化されている場合には、データ復号回路 116 の動作を復号動作とするとともに、付加情報 47 の鍵情報を格納するバックから、鍵情報を取得するようにし、暗号フラグが“0”の場合は、データ復号回路 116 の動作を、復号しないでそのまま出力するようにすることで、パケットデータが暗号化されていない場合の制御動作の簡略化が図れる。また、暗号フラグを鍵情報を格納するバックに格納する方法では、暗号フラグが“0”、すなわちパケットデータが暗号化されていない場合は、そのバックの 3 バイト目以降のブロック鍵情報は格納されていない。

【0071】その他、暗号フラグを用いずに、例えば、鍵情報を格納するバックの有無で暗号化されているかどうかを判別することもできる。

【0072】図 20 は図 2 の記録信号処理回路 102a および再生信号処理回路 102b からなるディジタル記録再生信号処理回路 102 の構成図である。400 はメモリ回路、401 は図 2 の制御回路 104 に従いメモリ回路 400 を制御するアドレス等を生成するメモリ制御回路、402 は C2 パリティ演算回路、403 は C1 パリティ演算回路、404 は前記制御回路 104 からの設定内容に従い記録時の ID 情報、サブコード生成、フォーマット情報、ブロック情報、鍵情報等の付加情報の付加、および再生時の ID 情報、サブコード、フォーマット情報、ブロック情報、鍵情報等の付加情報の取得等を行う付加情報処理回路、405 は記録時の変調処理及び再生時の復調処理を行う変復調回路である。本実施例では、一例として C2 パリティ演算を行うために 6 トラックのデータを必要とするため、メモリ回路 400 は少なくとも 6 トラック分のデータを蓄積する容量を備えるものとする。

【0073】記録時には、端子 411、413 を介して図 2 の制御回路 104 により、記録状態に設定される。図 2 のデータ暗号回路 115 で暗号化されたパケットデータが端子 410 から入力され、メモリ制御回路 401 の制御信号に従いメモリ回路 400 に蓄積される。C2 パリティ演算に必要なデータが蓄積された後、メモリ回路 400 から逐次読みだされ、C2 パリティ演算回路 402 に入力されて、所定の演算が行われる。C2 パリティ演算回路 402 で得られた演算結果は、メモリ回路 400 に蓄積される。一方、端子 413 を介して図 2 の制

御回路 104 からの設定に従い、付加情報処理回路 404 で、入力された暗号化パケットデータの鍵に対応した鍵情報等のバックデータが生成され、メモリ回路 400 に蓄積される。さらに前記した記録ブロックを構成するように、鍵情報等を含めメモリ回路 400 から読みだされたデータは、C1 パリティ演算回路 403 で C1 パリティを付加され、変復調回路 405 に入力される。変復調回路 405 で所定の変調処理された信号は、端子 414 を介して出力され、図 2 の記録再生アンプ 116、回転ヘッド 100 を介してテープ 111 上に記録される。

【0074】図 21 はデータ記録開始時における信号処理のタイミングを示す図である。図 21 (a) はデータ暗号化回路 115 から入力されるパケットデータ、図 21 (b) は、データ暗号化回路 115 が暗号化の際に用いたデータ鍵、図 21 (c) は、前述の C2 パリティ 43 の 6 トラック単位構成にあわせて、図 20 の C2 パリティ演算回路 402 での C2 パリティ演算サイクル (本実施例では 6 トラック) を示し、図 21 (d) は回転ヘッド 100 を介してテープ 111 に記録する記録信号を示している。図 21 の実施例では、記録開始が設定される時間  $t_1$  より前にあらかじめブロック鍵 A を生成し、データ鍵 K a を演算して、データ暗号化回路 115 に供給しておく。また、記録開始が設定される時間  $t_1$  前は、記録信号処理回路 102 a は入力信号に関らずパケット無しとみなして記録信号処理を行うように制御する。これにより、時間  $t_0$  に記録開始が設定されても、期間  $p_0$  のデータに対しての C2 パリティの演算は可能となる。

【0075】図 2 の制御回路 104 は、時間  $t_0$  で記録開始にした時の入力データの C2 パリティ演算サイクル  $s_0$  が終了して、前記第 2 の誤り訂正符号を構成する  $n$  トラック (本実施例では 6 トラック) の先頭から記録信号を出力する (図 21 (d)) ように制御する。また、データ鍵は、この C2 パリティの演算サイクルで更新される。例えば、時間  $t_2$  より前にブロック鍵 B を生成し、データ鍵 K b を演算してデータ暗号化回路 115 に供給しておき、時間  $t_2$  の時点でデータ暗号化回路 115 においてデータ鍵を K b に切り換える。通常、データ暗号化回路 115 は、その処理のため、パケットデータの入力から出力までの間に遅延時間が生じる。そこで、時間  $t_2$  からデータ暗号化回路 115 がパケットを暗号化処理することにより生じるデータ遅延時間分前の時点で、データ暗号化回路 115 に供給するデータ鍵を K b に切り換える。あるいは、データ鍵が切り換えられたパケットデータからは、次の演算サイクルの処理に先送りしてもよい。この実施例では、先頭部分に余分なデータが記録されるが、記録開始にする時間  $t_1$  のタイミングによらず、記録すべき信号に対し C2 パリティを付加し、上記 C2 パリティ演算サイクル単位で記録できる。また、再生時において、先頭の余分なデータ部分は、パ

ケット無しとみなして記録処理しているので、C2 パリティ演算に用いられるだけで、出力されることはない。

【0076】記録終了時には、前記記録再生信号処理回路 102 a の、テープ 111 への記録動作を、複数トラックのデータを用いて演算する C2 パリティの演算サイクル (本実施例では 6 トラック) 完結で行うように前記制御回路 104 で制御する。この制御方式により、記録開始、記録終了の切換えタイミングによらず、テープ 111 上の記録データに全て C2 パリティを付加し、C2 パリティの演算サイクル単位で鍵情報が更新されパケットデータが暗号化されるので、再生時には、C2 パリティ演算サイクル単位で再生でき、C2 パリティ演算が可能となるので、鍵情報のデータ信頼性も向上する。

【0077】図 22 は図 2 のテープ 111 上の鍵情報を示す図である。同図中、1111 から 1117 は、C2 パリティ演算サイクルである 6 トラック単位で示した記録トラックである。この図の場合、記録トラック 1111 から 1113 まだが、ブロック鍵 A、記録トラック 1114 から 1116 まだがブロック鍵 B をもとに暗号化されたパケットデータ、およびそれらに対応した鍵情報であるバックデータが格納される。また、記録トラック 1117 は暗号化されずに記録されたトラックである。この図のように、暗号化されたトラックと、暗号化されていないトラックが同一のテープ上に混在することも可能である。鍵情報の更新は、例えば、48 トラック、96 トラック等、 $m \times n$  トラック毎 ( $m$  は 1 以上の整数、 $n$  は本実施例では 6)、あるいは一つの番組全体等考えられるが、鍵の切り換わり目、あるいは暗号化されたトラックと、暗号化されていないトラックとの境目は、C2 パリティ演算サイクル (本実施例では 6 トラック) の区切り目である。

【0078】以上、記録の際の動作について説明した。ここで、鍵情報をサブコード領域 (図 9 の 7) に記録することも可能であるが、鍵情報を、各ブロックのヘッダ (図 12 の 44) の部分に格納し、各トラック上のデータ記憶領域 (図 9 の 7) に記録することで、アフレコ等による鍵情報のみの書き換えは困難となる。従って、鍵情報の消失を防ぐことができ、また、故意に鍵情報のみを改ざんして意図的に暗号通信を行うことはできない効果がある。

【0079】次に、テープからの再生方法について述べる。

【0080】図 20 のデジタル記録再生信号処理回路 102 において、再生時は、端子 411、413 を介して図 2 の制御回路 104 によって、再生状態に設定される。前記テープ 111 から回転ヘッド 100 で再生され、端子 414 から入力された再生信号は、変復調回路 405 で復調処理された後、C1 パリティ演算回路 403 で C1 パリティ演算を行い、誤り検出およびその訂正を行い、C1 パリティ演算結果と一緒にメモリ回路 40

0に蓄積される。C2パリティ演算に必要なデータが蓄積された後、メモリ制御回路401の制御信号に従いメモリ回路400から逐次読みだされ、C2パリティ演算回路402に入力される。C2パリティ演算回路402では、上記データで演算を行い、誤りの検出、訂正処理したデータおよびC2パリティ演算結果を、再びメモリ回路400に蓄積する。

【0081】図2のタイミング生成回路105から端子412を介して入力されるタイミング信号を基準として所定の順番にメモリ回路400からデータを読みだし、前記C1パリティ、C2パリティの演算結果を参照し、誤りの無いデータのみを端子410から図2の入出力制御回路119に出力する。一方、付加情報処理回路404では、メモリ回路400から読み出したデータから鍵情報やサブコード等を取得し、端子413を介して図2の制御回路104に送出する。その後、図8で示した演算、すなわち再生によって得られた鍵情報から、Kpを取り出し、デバイス鍵発生器117からのデバイス鍵との排他的論理和をとって、ハッシュ関数121の演算を行い、データ鍵を得、図2のデータ復号回路116に出力する。このデータ鍵は、記録時に用いたデータ鍵と同一のものであり、データ復号回路116において、正しくもとのパケットデータを得ることができる。

【0082】図23は、本発明のデータ再生時における信号処理のタイミングを示す図である。図23(a)は回転ヘッド100を介してテープ111から再生される再生信号、図23(b)は上記C2パリティの演算サイクル(本実施例では6トラック)を示し、図23(c)は入出力制御回路119から出力されるパケットデータを示し、図23(d)は、図2のデータ復号回路116に供給されるデータ鍵を示している。付加情報処理回路404では、演算サイクルs3においては、このサイクルで用いられている鍵情報KpCが検出されている。このKpCにより前述の演算で得られたデータ鍵Kcが、例えば前述のデータ鍵レジスタ1163aに記憶されており、データ鍵セクタ1169も、データ鍵レジスタ1163aのデータ鍵Kcが出力されるように選択されている。

【0083】次に、演算サイクルs4において、鍵情報KpDが用いられていることが検出されると、あらかじめ、データ鍵Kdを前述の演算で求めておき、データ鍵レジスタ1163bに記憶させ、時間t3のタイミングで、データ鍵セクタ1169を制御してデータ鍵レジスタ1163bのデータ鍵Kdに切り換える。以上の方法により、データ鍵を更新しながらの再生動作が可能となる。

【0084】また、既に記録済みのテープに追加記録する場合、C2パリティの付加単位の区切り目から、記録を開始するようにすることで、追加記録直前のトラックの鍵情報のデータ信頼性を損なわずに、つなぎ記録が可

能となる。

【0085】その他、パケットデータが暗号化されているかいないかを区別する方法としては、図4で示した同期バイト501は、通常固定データであるので、例えば、再生信号処理回路102bにおいて、この同期バイトの検出を行い、検出できた場合は、図2のデータ復号回路116を入力されるパケットデータを何もしないで通過させる機能に切り換え、検出できなかった場合は、図2のデータ復号回路116を復号機能の動作に切り換え、付加情報エリア内の鍵情報を検出する動作を行うことで、記録時に、パケットデータを暗号化して記録されたトラックと、暗号化しないで記録したトラックとが混在するテープの場合にも、検出が可能となる。

【0086】また、あらかじめ記録されているソフトテープについても、以上説明した方法で、ソフトテープの作成および再生が可能となり、テープ上のパケットデータの保護が実現できる。

【0087】以上は、記録トラックに現在のブロック鍵が格納されている例を示したが、データ鍵の演算は、C2の一演算サイクル内で行わなければならない。C2の一演算サイクル内でデータ鍵の演算が間に合わない場合は、前述のように、記録トラック内に、現在のブロック鍵と、次のブロック鍵を記録しておくことで、あらかじめ、次のデータ鍵を求めておける。

【0088】図24は図1のデジタル信号記録再生装置200の他の構成図である。同図中、121は、例えばIEEE1394のような高速デジタルバスインターフェース等のプロトコルを実現するデジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する、122は、デジタルインターフェースバスである。123は、デジタルインターフェース122上を伝送されるデジタルデータを保護するための暗号/復号回路であり、パケットデータを暗号化してデジタルインターフェースバス122上に伝送し、あるいは受信したデジタルデータを復号化する。124は、マイクロプロセッサのような制御回路であり、デジタルインターフェース回路121、暗号/復号回路123を制御する。

【0089】記録時には、デジタルインターフェースバス122上を伝送されてきた暗号化されたデジタルデータをデジタルインターフェース回路121において、所定のパケット処理を行い、暗号/復号回路123において、元のパケットデータに復号して、入出力回路107に出力する。その後、前述で説明したように、データ暗号回路115でパケットデータを暗号化し、テープ111上に記録する。再生時には、データ復号回路116において、再生したパケットデータを復号化して、入出力回路107から暗号/復号回路123に出力し、暗号/復号回路123において暗号化して、デジタル



インターフェース回路 121 から、デジタルインターフェースバス 122 に出力する。これによれば、テープ上のパケットデータ、デジタルインターフェースバス上のパケットデータの双方の保護が実現できる。

【0090】次に、光ディスクでの実施例を説明する。

【0091】図 25 は、ディスク上に記録されているファイルの構成図である。601 はリードイン領域であり、各種パラメータが格納されている。602、603、…は、プログラム 1 領域、プログラム 2 領域、…であり、各プログラム領域には、それぞれ異なる番組等が格納されている。

【0092】図 26 は、一つのプログラム領域例えばプログラム 1 領域の構成図である。プログラム領域は複数のユニットで構成され、この各ユニットに、例えば、後述するデジタル圧縮映像信号の一つの単位であるシーケンスを一個格納する。

【0093】図 27 は、デジタル圧縮映像信号のフレーム単位で圧縮されたイントラフレームデータと、前後のフレームのデータよりの予測を用いて差分情報のみの圧縮を行ったインターフレームデータの関係である。621 はイントラフレーム、622 はインターフレームである。デジタル圧縮映像信号は、所定数のフレーム、例えば 15 フレームを一つのシーケンスとし、その先頭はイントラフレーム 621 とし、残りのフレームはインターフレーム 622 としている。もちろん、先頭以外にもイントラフレーム 621 を配置するようにしてもよい。

【0094】図 28 は、デジタル圧縮映像信号の構成である。623 はフレーム単位で付加されるピクチャヘッダ、624 はシーケンス単位で付加されるシーケンスヘッダである。シーケンスヘッダ 624 は、同期信号及び伝送レート等の情報により構成される。ピクチャヘッダ 623 は、同期信号及びイントラフレームかインターフレームかの識別情報等により構成される。通常、各データの長さは情報量により変化する。前述の一つのユニットに 1 シーケンスが格納される。

【0095】前述図 26 の各ユニットは、複数のデータセクタにより構成される。

【0096】図 29 は各データセクタの構成図である。631 は ID 情報で 4 バイト、632 は ID 情報 631 の誤り検出訂正のためのパリティで 2 バイト、633 は管理データで 6 バイト、634 はユーザデータで 2048 バイト、635 はユーザデータ 634 の誤り検出訂正のためのパリティで 4 バイトから構成される。このうちユーザデータ 634 に、図 28 で示したデジタル圧縮映像信号が、分割され格納される。その他、デジタル圧縮音声圧縮信号も、分割されユーザデータ 634 に格納される。前述の一つのユニットは、デジタル圧縮映像信号、音声信号が、それぞれ格納されたデータセクタの集まりである。

【0097】図 30 は、ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。まず、データセクタが 172 バイトに区切られ、それに対し、10 バイトの第 1 の誤り検出訂正のためのパリティ 637 の一部 (C1 パリティパリティ 637 の一部) が付加される。さらにこのデータセクタを n 個 (例えば本実施例では 16 個) 集め、今度は行方向の 192 バイトに 16 個の第 2 の誤り検出訂正のためのパリティ 636 (C2 パリティ 636) が付加される。得られた C2 パリティ 636 にも 10 バイトの C1 パリティ 637 の一部が付加される。

【0098】図 31 は、光ディスクを記録媒体として用いたデジタル信号記録再生装置の構成図である。同図中、701 は光ディスク、702 は光ピックアップ、703a は記録時の記録信号の生成等を行う記録信号処理回路、703b は再生時の再生信号の復調等を行う再生信号処理回路、704 はマイクロプロセッサのような制御回路、705 はスピンドルモータ、706 は光ディスク 701 の回転速度および光ピックアップ 702 の位置、焦点を制御するサーボ回路、709 は図 6 と同様の項構成のデジタル信号記録時のデータ暗号回路、710 は図 19 と同様の構成のデジタル信号再生時のデータ復号回路、711 は、デジタル信号を暗号あるいは復号する際にデータ暗号回路 709 あるいはデータ復号回路 710 に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、712 はデジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるディスク鍵を発生するディスク鍵発生器、713 はデジタル情報を暗号あるいは復号する際のデータ鍵のさらにもう一つのもとであるブロック鍵を発生するブロック鍵発生器、719 はデジタルインターフェース回路、720 は入出力端子である。

【0099】記録時には、入出力端子 720 から、図 29 のデータセクタのユーザデータ 634 の形式に区切られたデジタル圧縮映像信号等のデジタル信号が、デジタルインターフェース回路 719 に入力される。入力されたデジタル信号は、データ暗号回路 709 において、デバイス鍵発生器 711、ディスク鍵発生器 712 およびブロック鍵発生器 713 により発生される鍵とともに制御回路 704 において生成されるデータ鍵によって、入力されたデジタル信号を暗号化し、これを記録信号処理回路 703a に出力する。記録信号処理回路 703a では、入力されたユーザデータ形式のデジタル信号に、図 29 の ID 631、パリティ 632、管理データ 633、およびパリティ 635 を付加し、データセクタの形式にする。次に、n 個のデータセクタを単位として (本実施例では 16 個)、図 30 の C1 パリティ 637、C2 パリティ 636 を付加し、さらに図示しないが、所定の並べ替え、ヘッダを付加し、変調処理が施され、光ピックアップ 702 を介して光ディスク 701 上

に記録される。

【0100】図32は、データ暗号回路709に供給するデータ鍵の生成例であり、例えば、これらの生成は、図31の制御回路704内にて行われる。デバイス鍵発生器711は、例えば96ビットのあらかじめ定められた固定の鍵情報を記憶している。ディスク鍵発生器712、ブロック鍵発生器713は、例えば図31の制御回路704からの司令7121、7131により96ビットの乱数を発生させる乱数発生器である。721、722は96ビットの排他的論理和演算器、723はハッシュ関数演算器である。まず、ブロック鍵は、ハッシュ関数演算器723にてハッシュ演算がなされ、その結果のうちの56ビットが、データ鍵として図31のデータ暗号回路709に供給される。また、96ビットのブロック鍵は、96ビットのディスク鍵と排他的論理和演算器722にて排他的論理和がとられ（以下鍵情報K<sub>r</sub>という）、図31の記録信号処理回路703aに送られ、光ディスク701上に記録される。さらに、ディスク鍵とデバイス鍵とが排他的論理和演算器721で排他的論理和がとられ（以下鍵情報k<sub>d</sub>という）、図31の記録信号処理回路703aに送られ、光ピックアップ702を介して、光ディスク701上に記録される。

【0101】ここで、図31の制御回路704からの司令7131を、ある時間間隔で発生させ、上述の演算によるデータ鍵の生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、光ディスク上のデータの安全性を高めることが可能となる。また、司令7121は、例えば一回の記録動作の際に一回発生させる。あるいは、空の光ディスクに最初に記録する際に一回だけ発生させてk<sub>d</sub>を記録し、次の記録動作からは、一旦光ディスク上の前述の鍵情報k<sub>d</sub>を再生し、デバイス鍵と排他的論理和をとることで得られるディスク鍵を用いてブロック鍵と排他的論理和をとり鍵情報k<sub>r</sub>を得る方法もある。さらに、ディスク鍵発生器712を用いず、光ディスクの製造過程であらかじめ鍵情報k<sub>d</sub>を記録しておき、記録動作の前にそのk<sub>d</sub>を再生し、ディスク鍵を得るという方法もある。鍵情報k<sub>d</sub>は、例えば図25のリードイン領域601に記録される。

【0102】再生の際には、まず鍵情報k<sub>d</sub>を再生し、鍵情報k<sub>d</sub>とデバイス鍵とを排他的論理和をとることでディスク鍵を得、さらに再生した鍵情報k<sub>r</sub>と、得られたディスク鍵とを排他的論理和をとってブロック鍵を得、ハッシュ関数723の演算を行うことで、図31のデータ復号回路710に入力するデータ鍵を得る。

【0103】図31において、再生の際には、光ピックアップ702より再生された再生信号が再生信号処理回路703bに入力され、再生信号処理回路703bにおいて復調及び誤り検出訂正を行うとともに、図29のユーザデータ634の形式のデジタル信号が、データ復号回路710に出力される。再生信号処理回路703b

ではディスク鍵、ブロック鍵情報の再生も行い、制御回路704に送る。制御回路704においては、前述のデータ鍵再生の演算を行ってデータ復号回路710に供給する。データ復号回路710において再生信号処理回路703bからのデジタル信号が復号され、デジタルインターフェース回路719を介して入出力端子720から出力される。

【0104】なお、記録するデジタル信号を保護する必要がない場合は、暗号化しないでそのまま光ディスクに記録してもよい。

【0105】図33は、図29の管理データ633の構成図である。この管理データ633に、前述の鍵情報k<sub>r</sub>を格納する。6341はこの管理データ633が格納されているデータセクタのユーザデータが暗号化されているかどうかを示す暗号フラグ、6342はこの管理データに格納されている鍵情報が有効か無効かを示すデータ有効フラグ、6343は鍵情報k<sub>r</sub>が一つの管理データ633に格納できない場合、後続の管理データがあることを示す鍵シーケンス番号、6344は鍵情報k<sub>r</sub>である。

【0106】図34は、鍵情報k<sub>r</sub>を図29の管理データ633の領域に格納する方法を示す図である。この例では、図30のC2パリティ636の付加単位である16個のデータセクタ（データセクタ0～データセクタ015）の管理データを一つの単位として、前述の64ビットの鍵情報を格納する。96ビットの鍵情報k<sub>r</sub>は3個の管理データにk<sub>r</sub>0、k<sub>r</sub>1、k<sub>r</sub>2に分割され格納される。その際、暗号フラグ6341は暗号化されていることを示す“1”が、データ有効フラグは有効であることを示す“1”が、また、鍵シーケンス番号6343は、3個の管理データに順に2、1、0を格納し、0が分割の最後であることを示す。これらが、16個の管理データに繰り返し格納される。ただし、最後の管理データは、半端となるので、データ有効フラグは無効であることを示す“0”が、格納される。

【0107】以上のように、鍵情報が光ディスク上に記録される。この時、鍵情報は16個またはその整数倍のデータセクタを単位として更新される。この鍵情報の更新は、64データセクタ、128データセクタ等、m×nデータセクタ毎（mは1以上の整数、nは本実施例では16）等に行うことが考えられるが、鍵の切り換わり目、あるいは暗号化の有無の境目は、C2パリティの付加単位（本実施例では16データセクタ）の区切り目である。このことにより、再生時にC2パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【0108】なお、記録信号処理回路703a、再生信号処理回路703bは、図20のデジタル記録再生信号処理回路102の動作と同様の動作を行う。ただし、C2パリティの付加単位は、nデータセクタ単位（本実施例では16データセクタ）となる。



【0109】図35は、光ディスクを記録媒体として用いたデジタル信号記録再生装置の他の構成図である。本実施例では、図3に示したデジタル映像圧縮信号の固定長の packets を光ディスク701に記録再生する場合の例である。図35中、717は、例えばIEEE1394のような高速デジタルバスインターフェース等のプロトコルを実現するデジタルインターフェース回路であり、入力された packets データの時間間隔を維持しながら、高速にデータを伝送する機能を有する。718は、デジタルインターフェースバスである。715はデジタルインターフェース718上を伝送されるデジタルデータを保護するための暗号/復号回路であり、 packets データを暗号化してデジタルインターフェースバス718上に伝送し、あるいは受信したデジタルデータを復号化する。716は、マイクロプロセッサのような制御回路であり、デジタルインターフェース回路717、暗号/復号回路715を制御する。707は packets データをデータセクタのユーザデータに変換、あるいはユーザデータから packets データを取り出すセクタ変換回路、708は記録時の packets データへのタイムスタンプ処理、再生時の packets データの出力制御を行う入出力制御回路である。

【0110】記録時には、デジタルインターフェース回路717において、デジタルインターフェースバス718上を伝送されてきた暗号化されたデジタルデータに所定の packets 処理を行い、暗号/復号回路715において、元の packets データに復号して、入出力回路714に出力する。その後、データ暗号回路709で packets データを暗号化し、入出力制御回路708において入力された packets データにタイムスタンプを施し、セクタ変換回路707に出力する。セクタ変換回路707では、入力された packets データを前述のデータセクタのユーザデータの形式に変換する。ユーザデータの形式に変換されたデジタル信号が、記録信号処理回路703a及び光ピックアップ702を介して、光ディスク701上に記録される。

【0111】したがって、光ディスク701上には、鍵情報に所定の演算を行って得られた鍵で暗号化された前記デジタル信号と共に、前記鍵情報が、所定の領域に記録されている。また前記デジタル信号は、所定長の packets 形式を有してなる。さらに、前記鍵情報が所定間隔で更新され、所定の領域に記録されている。またさらに、複数種類の鍵で変換された変換デジタル信号および前記鍵が記録されている。

【0112】再生時には、光ピックアップ702及び記録信号処理回路703aを介して、セクタ変換回路707において、再生したユーザデータから packets データを取り出し、入出力制御回路708において記録時に付加されたタイムスタンプをもとに出力タイミングを制御しタイムスタンプが取り除かれた packets データが出力

される。さらに、データ復号回路710において、再生した packets データを復号化して、入出力回路714から暗号/復号回路715に出力し、暗号/復号回路715において暗号化して、デジタルインターフェース回路717から、デジタルインターフェースバス718に出力する。

【0113】図36は、図35のセクタ変換回路707によって変換された図29のデータセクタのユーザデータ634に格納される packets データの構成図である。デジタル映像圧縮信号の固定長の packets が複数個格納される。図35の入出力制御回路708において、各 packets 643, 645, …には、例えば4バイトの時間情報642, 644, …が付加される。データセクタが2048バイトの場合、時間情報が付加された10個の packets が格納可能である。時間情報が付加された packets は、連続して格納される必要はなく、途中に未使用領域があってもよい。また、 packets ヘッド641を付加することで、 packets の区切り目を容易に判別することができる。

【0114】本実施例においても、前述の鍵情報を切り換えるタイミング、あるいは暗号化の有無の境目としては、このC2パリティの付加単位であるnデータセクタ（本実施例では16データセクタ）の区切り目とすることで、再生時にC2パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

【0115】図37は、図36の各時間情報642, 644, …の構成図である。暗号フラグ651は、 packets が暗号化されているかどうかを示すフラグであり、鍵フラグは、この packets が暗号化されている場合、どの鍵で暗号化されているかを示すフラグである。例えば、このフラグを2ビットとして、鍵が更新される度に0、1、2、3と1ずつ増加する値をとり、同様のフラグを図29の管理データにも格納しておくことで、各 packets 毎に対応する鍵を明示することができる。これらのフラグは、前述の packets ヘッド641に格納してもよい。この方法によれば、 packets 毎に任意に鍵を更新することが可能となる。

【0116】なお、以上の実施例では、磁気テープおよび光ディスクでの記録再生について説明したが、磁気ディスクや、半導体メモリ等、他のあらゆる記録媒体に記録再生する場合でも、同様に適用することができる。

【0117】上記半導体メモリの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えば半導体メモリの記録の一つの単位であるアドレスの区切り目で行うとよい。

【0118】また、本実施例は、本発明を、デジタル信号を鍵により暗号化するシステムに適用したものである。しかし、本発明はこの実施例に限定されるものではなく、例えば、デジタル信号がキーコードによりスクランブルされたりするシステムにも適用可能である。す

なわち、本発明は、少なくとも、デジタル信号が元々のクリアな状態から変換されるように処理されるあらゆるシステムに対して適用可能なものである。

#### 【0119】

【発明の効果】本発明によれば、デジタル信号を、記録媒体上に記録または再生するデジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、デジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したデジタル信号を復号化して出力する。以上により、再生の際には、前記所定の演算を施さない限り、前記鍵が得られないので、記録媒体上の鍵情報を得ても、それを用いて暗号化されたデジタル信号を復号することは困難であり、記録媒体上のデジタル信号の著作権を保護することができる。

#### 【図面の簡単な説明】

【図1】本発明の実施例で、デジタル放送受信機とデジタル信号記録再生装置を含む構成図である。

【図2】図1のデジタル信号記録再生装置200の構成図である。

【図3】デジタル映像圧縮信号のパケットの構成図である。

【図4】図3のパケットヘッダ306の構成図である。

【図5】デジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。

【図6】図2のデータ暗号回路115の構成図である。

【図7】図6の暗号器1155の構成図である。

【図8】図2のデータ暗号回路115、データ復号回路116に供給するデータ鍵の生成例を示すところの制御回路104内のデータ鍵の生成図である。

【図9】テープ111の1トラックの記録パターンを示す図である。

【図10】図9のデータ記録領域7のブロックの構成図である。

【図11】図10のID情報21の構成図である。

【図12】図9のデータ記録領域7の1トラック分のデータの構成図である。

【図13】188バイトのパケット形式で伝送されたデジタル圧縮映像信号を、図12のデータ41に記録する時の1パケットのブロックの構成図である。

【図14】図12のデータ記録領域7のヘッダ44の構成図である。

【図15】図14の付加情報47の領域に、ブロック鍵を格納する場合のバックデータの構成図である。

【図16】ブロック鍵の格納方法を示す図である。

【図17】ブロック鍵の他の格納方法を示す図である。

【図18】図13の時間情報25の具体的構成図である。

【図19】図2のデータ復号回路116の構成図である。

【図20】図2の記録信号処理回路102aおよび再生信号処理回路102bからなるデジタル記録再生信号処理回路102の構成図である。

【図21】データ記録開始時における信号処理のタイミングを示す図である。

【図22】図2のテープ111上の鍵情報を示す図である。

【図23】データ再生時における信号処理のタイミングを示す図である。

【図24】図1のデジタル信号記録再生装置200の他の構成図である。

【図25】ディスク上に記録されているファイルの構成図である。

【図26】一つのプログラム領域の構成図である。

【図27】デジタル圧縮映像信号のイントラフレームデータとインターフレームデータの関係を示す図である。

【図28】デジタル圧縮映像信号の構成図である。

【図29】データセクタの構成図である。

【図30】ディスクにデータセクタを記録する際に付加する誤り訂正符号を付加した構成図である。

【図31】光ディスクを記録媒体として用いたデジタル信号記録再生装置の構成図である。

【図32】データ暗号回路709に供給するデータ鍵の生成例を示す図である。

【図33】図29の管理データ633の構成図である。

【図34】鍵情報krを管理データ領域に格納する方法を示す図である。

【図35】光ディスクを記録媒体として用いたデジタル信号記録再生装置の他の構成図である。

【図36】図29のデータセクタのユーザデータ634に格納されるパケットデータの構成図である。

【図37】暗号フラグ等を前述の時間情報に付加する場合の時間情報の構成図である。

#### 【符号の説明】

7…データ記録領域、20…同期信号、21…ID情報、22…データ、25…時間情報、31…グループ番号、32…トラックアドレス、33…ブロックアドレス、41…映像信号データ、44…ヘッダ、45…フォーマット情報、46…ブロック情報、47…付加情報、71…パケット、100…回転ヘッド、101…キャプスタン、102a…記録信号処理回路、102b…再生信号処理回路、104…制御回路、105…タイミング生成回路、106…サーボ回路、107…入出力回路、109…タイミング制御回路、110…発振回路、115…データ暗号回路、116…データ復号回路、117…デバイス鍵発生器、118…ブロック鍵発生器、119…入出力制御回路、200…デジタル信号記録再生

31

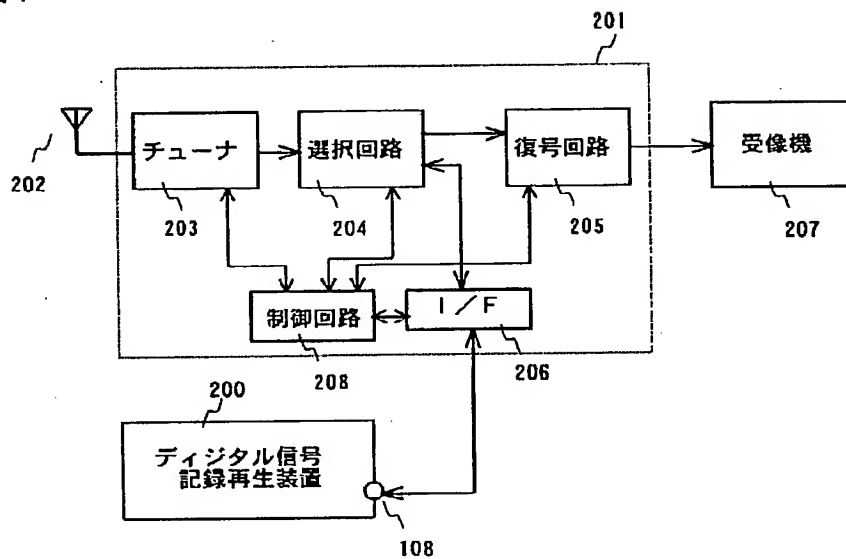
装置、201…デジタル放送受信機、203…チューナ、204…選択回路、205…復号回路、206…インターフェース回路、208…制御回路、1152…ブロック処理回路、1154…鍵スケジュール回路、1155…暗号器、1158…データ鍵レジスタ、1159…データ鍵セレクタ、1165…復号器、400…メモリ回路、401…メモリ制御回路、402…C2パリティ演算回路、403…C1パリティ演算回路、404…付加情報処理回路、405…変復調回路、551…暗号

32

処理部。701…光ディスク、702…光ピックアップ、703a…記録信号処理回路、703b…再生信号処理回路、704…制御回路、705…スピンドルモータ、706…サーボ回路、707…セクタ変換回路、708…入出力制御回路、709…データ暗号回路、710…データ復号回路、711…デバイス鍵発生器、712…ディスク鍵発生器、713…ブロック鍵発生器、719…デジタルインターフェース回路。

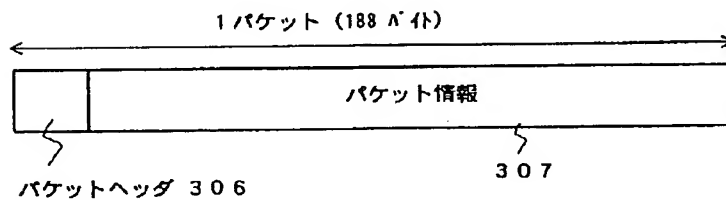
【図1】

図1



【図3】

図3



【図14】

図14

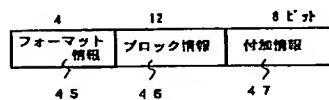
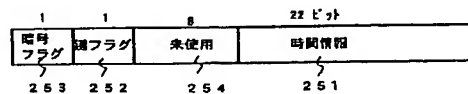
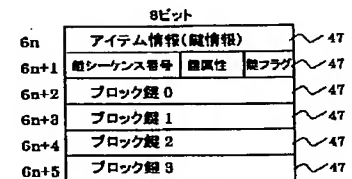


図18



【図15】

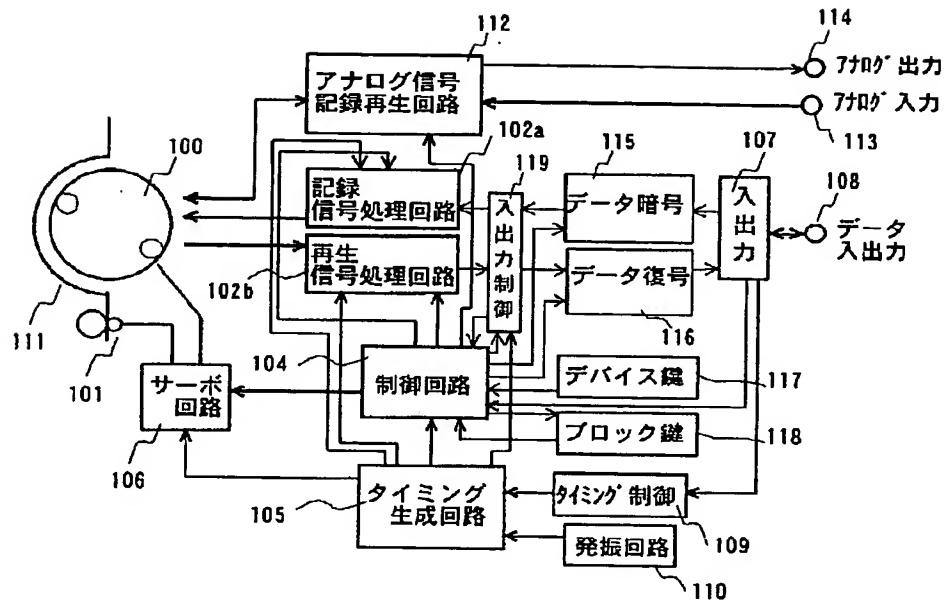
図15



【図18】

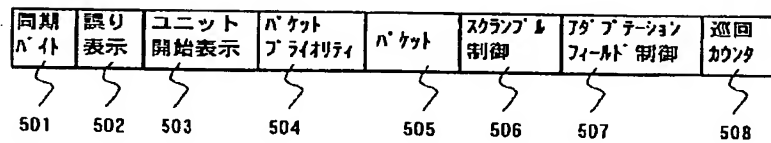
【図2】

図2



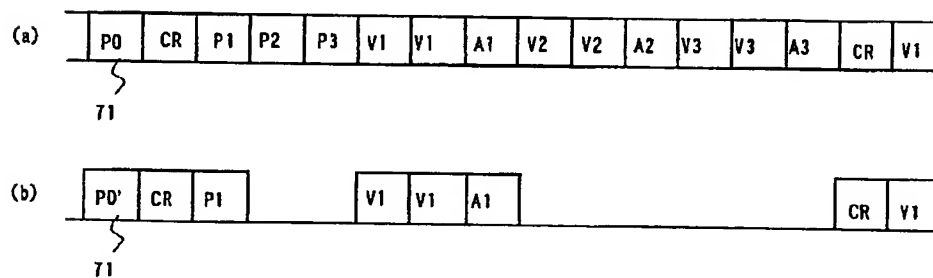
【図4】

図4



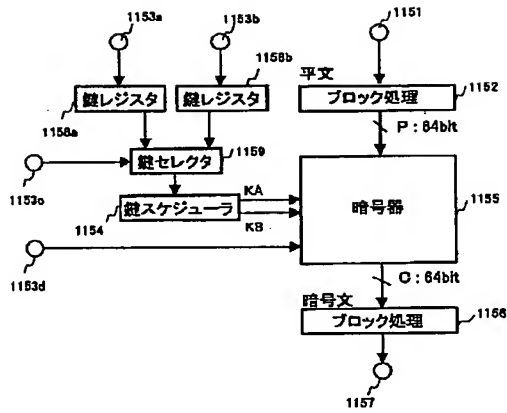
【図5】

図5



【図6】

図6



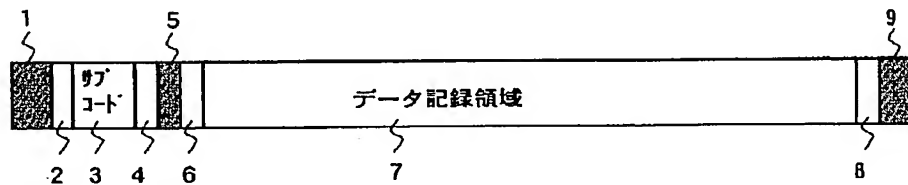
【図25】

図25



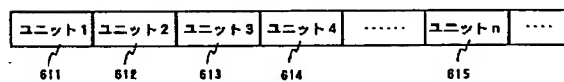
【図9】

図9



【図26】

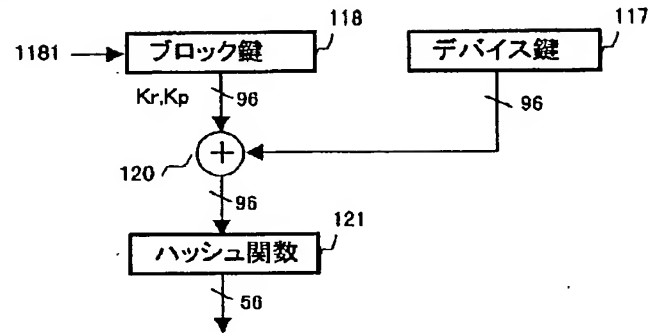
図26



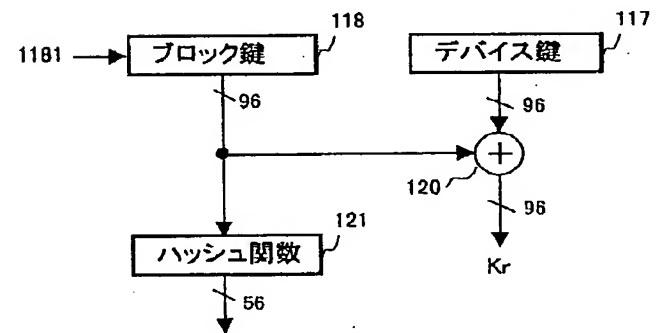
【図8】

図8

(a)

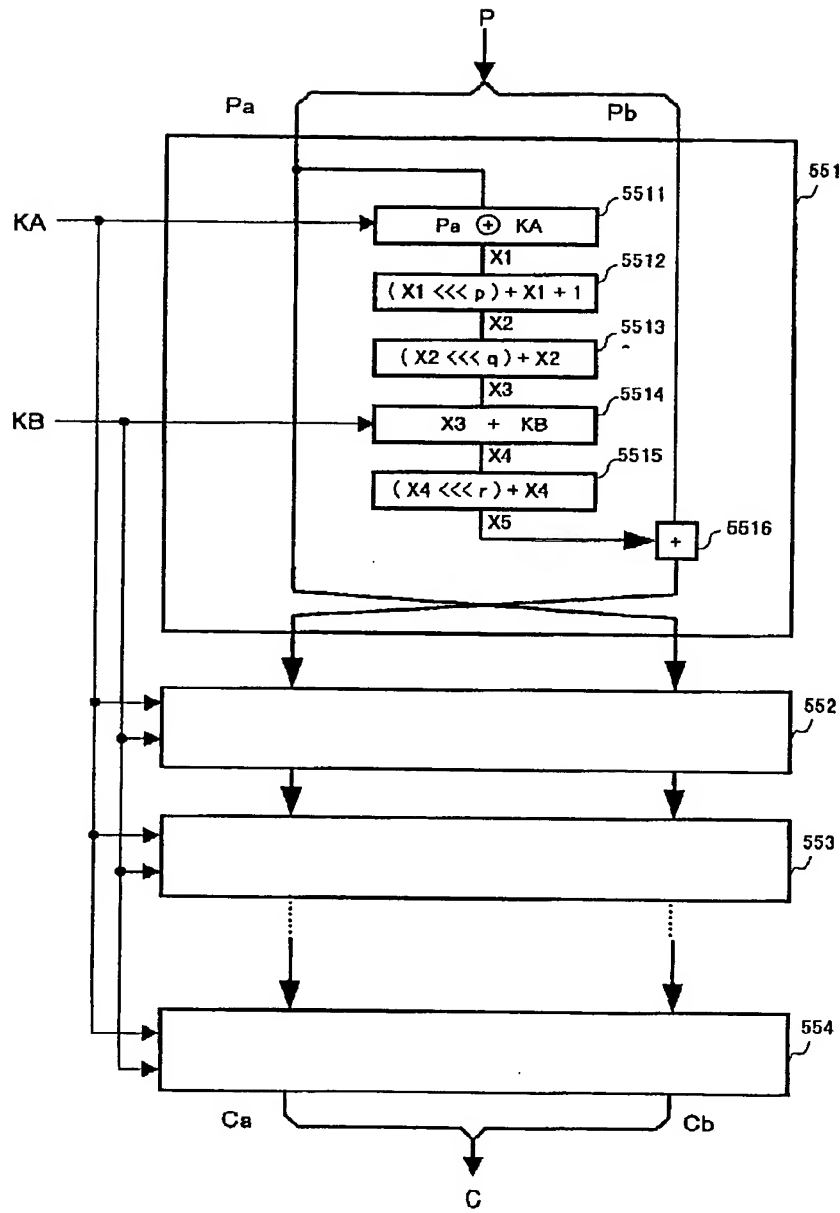


(b)



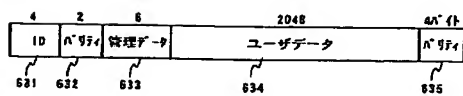
【図 7】

図 7



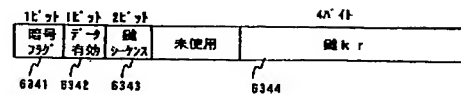
【図 29】

図 29



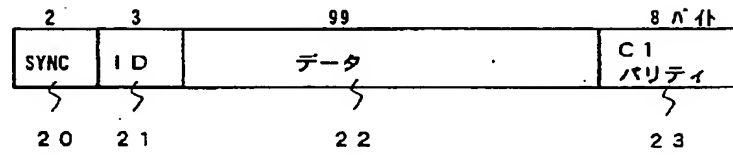
【図 33】

図 33



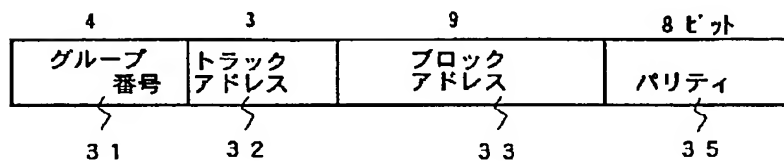
【図10】

図10



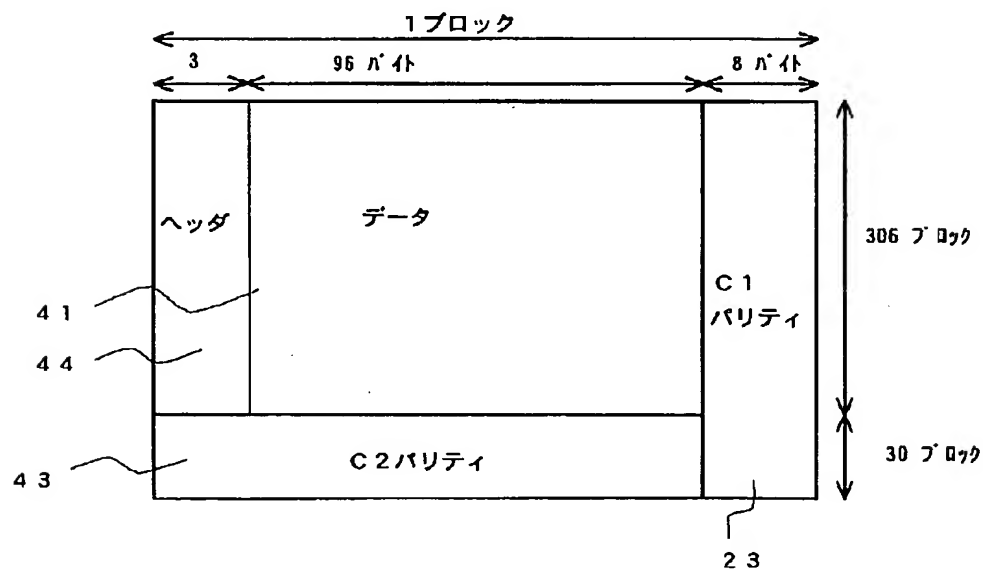
【図11】

図11



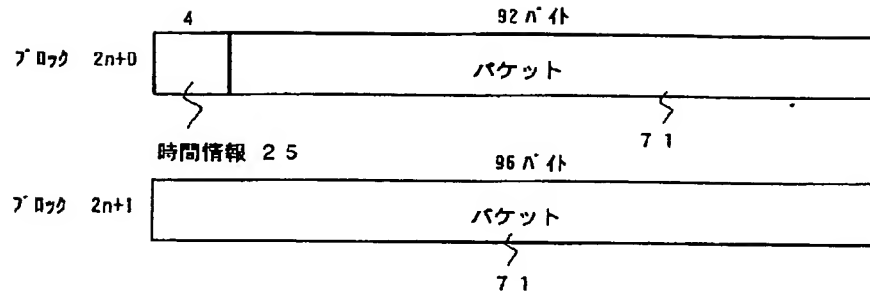
【図12】

図12



【図 13】

図 13



【図 16】

図 16

(1)

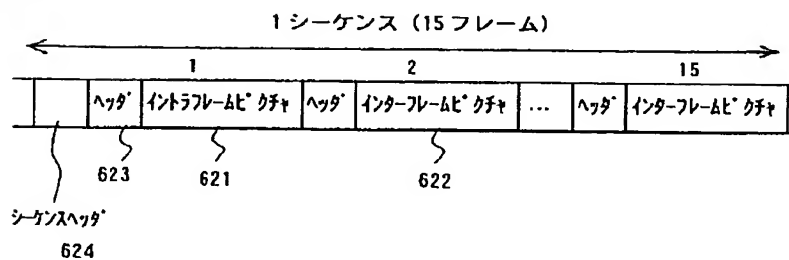
6a	“鍵情報”	6b	“鍵情報”	6c	“鍵情報”
6a+1	“2” “0” “0”	6b+1	“1” “0” “0”	6c+1	“0” “0” “0”
6a+2	ブロック鍵 A0	6b+2	ブロック鍵 A4	6c+2	ブロック鍵 A8
6a+3	ブロック鍵 A1	6b+3	ブロック鍵 A5	6c+3	ブロック鍵 A9
6a+4	ブロック鍵 A2	6b+4	ブロック鍵 A6	6c+4	ブロック鍵 A10
6a+5	ブロック鍵 A3	6b+5	ブロック鍵 A7	6c+5	ブロック鍵 A11

(2)

6d	“鍵情報”	6e	“鍵情報”	6f	“鍵情報”
6d+1	“2” “0” “1”	6e+1	“1” “0” “1”	6f+1	“0” “0” “1”
6d+2	ブロック鍵 B0	6e+2	ブロック鍵 B4	6f+2	ブロック鍵 B8
6d+3	ブロック鍵 B1	6e+3	ブロック鍵 B5	6f+3	ブロック鍵 B9
6d+4	ブロック鍵 B2	6e+4	ブロック鍵 B6	6f+4	ブロック鍵 B10
6d+5	ブロック鍵 B3	6e+5	ブロック鍵 B7	6f+5	ブロック鍵 B11

【図 28】

図 28





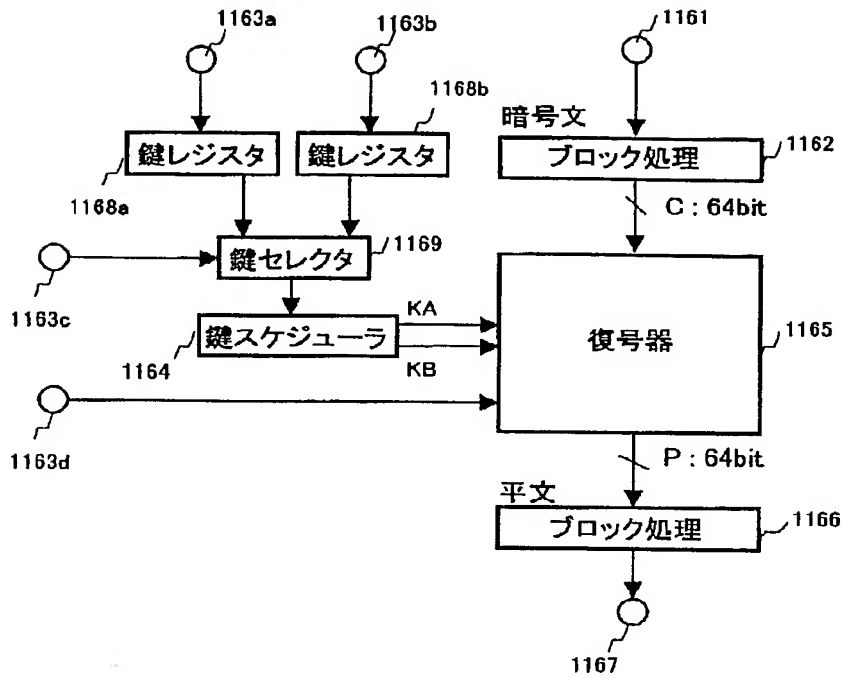
【図 17】

図 17

(1)	6a	“鍵情報”	6b	“鍵情報”	6c	“鍵情報”
	6a+1	“2” “0” “0”	6b+1	“1” “0” “0”	6c+1	“0” “0” “0”
	6a+2	ブロック鍵 A0	6b+2	ブロック鍵 A4	6c+2	ブロック鍵 A8
	6a+3	ブロック鍵 A1	6b+3	ブロック鍵 A5	6c+3	ブロック鍵 A9
	6a+4	ブロック鍵 A2	6b+4	ブロック鍵 A6	6c+4	ブロック鍵 A10
	6a+5	ブロック鍵 A3	6b+5	ブロック鍵 A7	6c+5	ブロック鍵 A11
(2)	6d	“鍵情報”	6e	“鍵情報”	6f	“鍵情報”
	6d+1	“2” “1” “1”	6e+1	“1” “1” “1”	6f+1	“0” “1” “1”
	6d+2	ブロック鍵 B0	6e+2	ブロック鍵 B4	6f+2	ブロック鍵 B8
	6d+3	ブロック鍵 B1	6e+3	ブロック鍵 B5	6f+3	ブロック鍵 B9
	6d+4	ブロック鍵 B2	6e+4	ブロック鍵 B6	6f+4	ブロック鍵 B10
	6d+5	ブロック鍵 B3	6e+5	ブロック鍵 B7	6f+5	ブロック鍵 B11
(3)	6a	“鍵情報”	6b	“鍵情報”	6c	“鍵情報”
	6a+1	“2” “0” “1”	6b+1	“1” “0” “1”	6c+1	“0” “0” “1”
	6a+2	ブロック鍵 B0	6b+2	ブロック鍵 B4	6c+2	ブロック鍵 B8
	6a+3	ブロック鍵 B1	6b+3	ブロック鍵 B5	6c+3	ブロック鍵 B9
	6a+4	ブロック鍵 B2	6b+4	ブロック鍵 B6	6c+4	ブロック鍵 B10
	6a+5	ブロック鍵 B3	6b+5	ブロック鍵 B7	6c+5	ブロック鍵 B11
(4)	6d	“鍵情報”	6e	“鍵情報”	6f	“鍵情報”
	6d+1	“2” “1” “0”	6e+1	“1” “1” “0”	6f+1	“0” “0” “0”
	6d+2	ブロック鍵 C0	6e+2	ブロック鍵 C4	6f+2	ブロック鍵 C8
	6d+3	ブロック鍵 C1	6e+3	ブロック鍵 C5	6f+3	ブロック鍵 C9
	6d+4	ブロック鍵 C2	6e+4	ブロック鍵 C6	6f+4	ブロック鍵 C10
	6d+5	ブロック鍵 C3	6e+5	ブロック鍵 C7	6f+5	ブロック鍵 C11

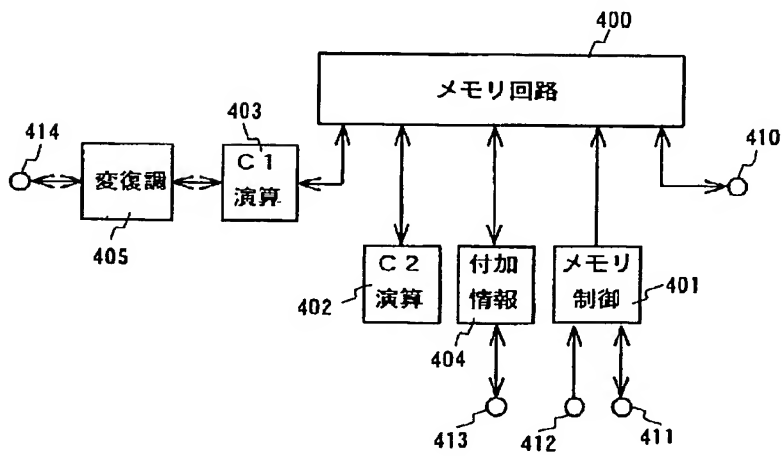
【図 19】

図 19



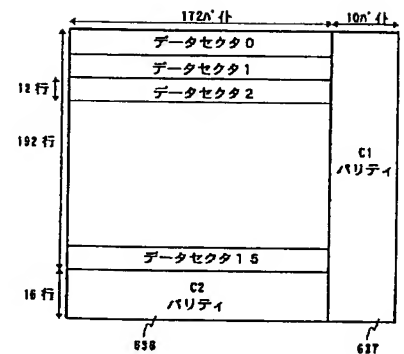
【図 20】

図 20



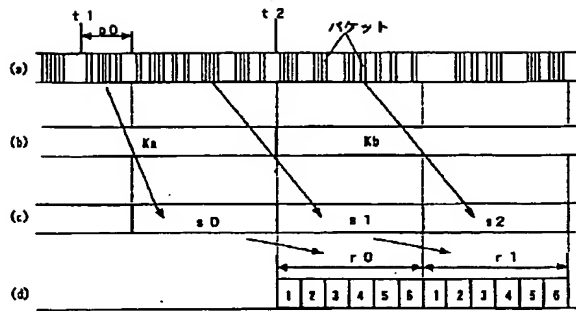
【図 30】

図 30



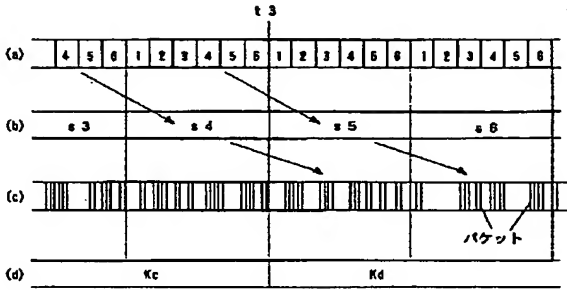
【図 2 1】

図 2 1



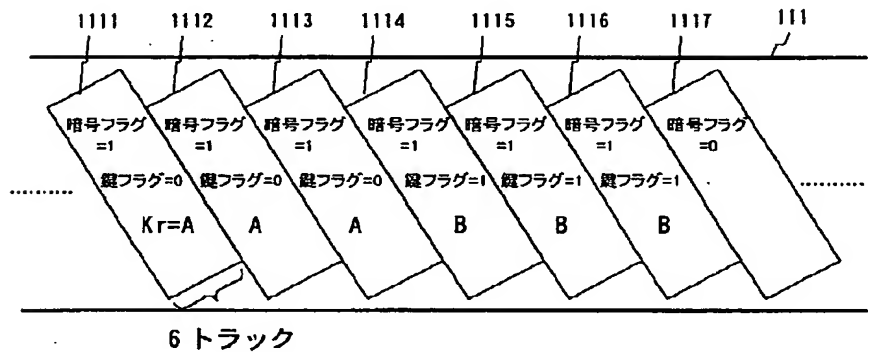
【図 2 3】

図 2 3



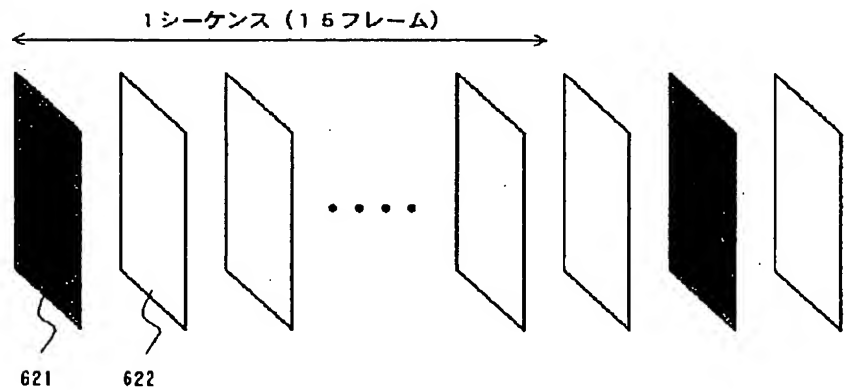
【図 2 2】

図 2 2



【図 2 7】

図 2 7



BEST AVAILABLE COPY

图 24

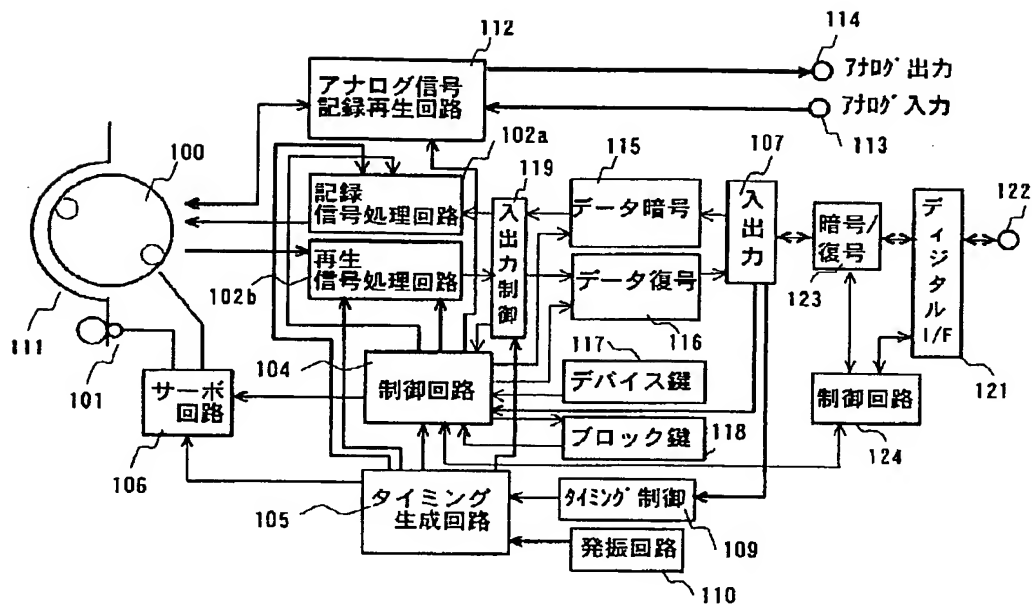


图 3 1

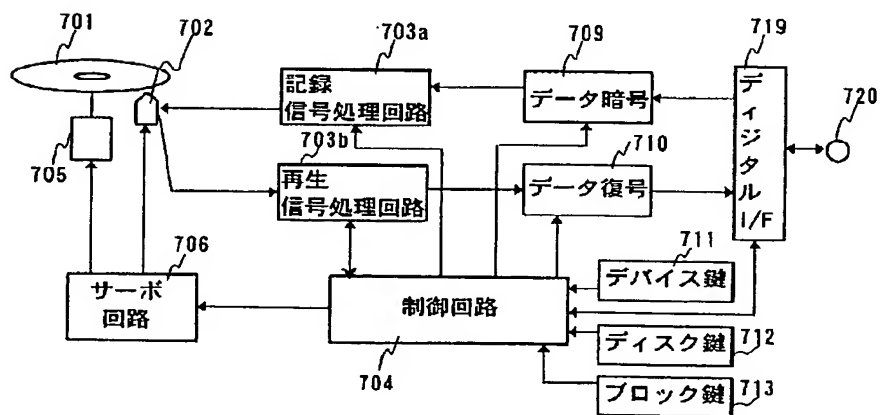
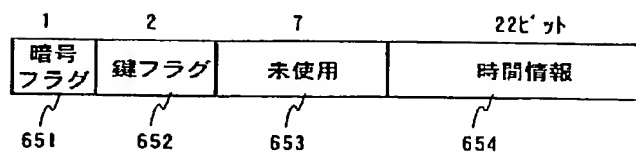
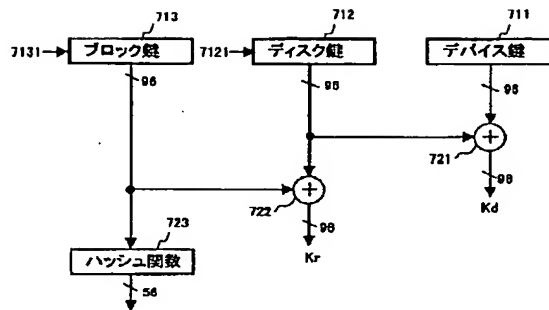


图 3 7



【図 32】

図 32



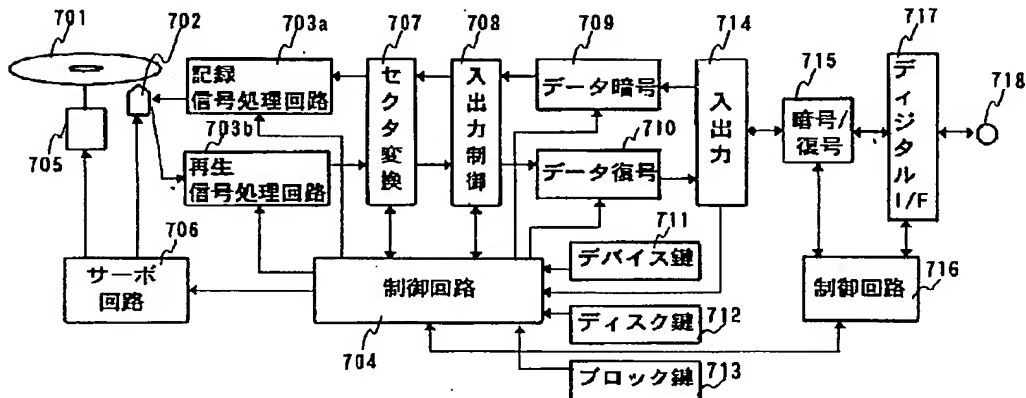
【図 34】

図 34

	6341	6342	6343	6344
(1)	"1"	"1"	"2"	未使用
(2)	"1"	"1"	"1"	未使用
(3)	"1"	"1"	"0"	未使用
(4)	"1"	"1"	"2"	未使用
(5)	"1"	"1"	"1"	未使用
...				
(15)	"1"	"1"	"0"	未使用
(16)	"1"	"0"	無効	未使用
				無効

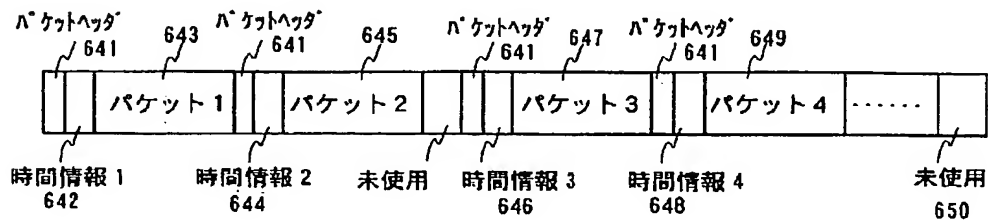
【図 35】

図 35



【図 36】

図 36



フロントページの続き

(72)発明者 千葉 浩

神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内

F ターム(参考) 5C053 FA13 FA20 FA22 FA23 GB01  
GB06 GB07 GB11 GB15 GB21  
GB30 GB37 JA21 JA22 JA26  
KA01 KA08 KA21 KA22 KA24  
LA06 LA07

(72)発明者 尾鷲 仁朗

神奈川県横浜市戸塚区吉田町292番地株式  
会社日立製作所マルチメディアシステム開  
発本部内

5D044 AB05 AB07 DE03 DE48 DE50  
DE52 DE60 DE68 GK08 GK17